Titre: Title:	A Location Routing Protocol Based on Smart Antennas for Wireless Sensor Networks
Auteur: Author:	Nelly Polo
Date:	2010
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Polo, N. (2010). A Location Routing Protocol Based on Smart Antennas for Wireless Sensor Networks [Mémoire de maîtrise, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/319/

URL de PolyPublie: PolyPublie URL:	https://publications.polymtl.ca/319/
Directeurs de recherche: Advisors:	Alejandro Quintero, & Samuel Pierre
Programme: Program:	Génie informatique

UNIVERSITÉ DE MONTRÉAL

A LOCATION ROUTING PROTOCOL BASED ON SMART ANTENNAS FOR WIRELESS SENSOR NETWORKS

NELLY POLO

DÉPARTEMENT DE GÉNIE INFORMATIQUE ET GÉNIE LOGICIEL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION

DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES

(GÉNIE INFORMATIQUE)

JUIN 2010

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé:

A LOCATION ROUTING PROTOCOL BASED ON SMART ANTENNAS FOR WIRELESS SENSOR NETWORKS

présenté par : POLO Nelly

en vue de l'obtention du diplôme de : Maîtrise ès sciences appliquées

a été dûment accepté par le jury d'examen constitué de :

Mme BOUCHENEB Hanifa, Doctorat, présidente

M.QUINTERO Alejandro, Doct, membre et directeur de recherche

M.PIERRE Samuel, Ph.D., membre et codirecteur de recherche

Mme NICOLESCU Gabriela, Doct, membre

ACKNOWLEDGEMENTS

First of all I would like to thank God, who guides me in my everyday life and activities.

I would like to thank my director of research, Mr. Alejandro Quintero for his support, patience, encouragement and good advice. Also, I would like to thank Mr. Samuel Pierre, my co-director or research, for welcoming me into LARIM (Laboratoire de recherche en réseautique et informatique mobile) and for his availability.

I owe my deepest gratitude to me fellow colleague and friend Luis Cobo for all his support, help, encouragement and advice, without whom none of this would have been possible.

I would like to thank my parents, my brother and my sister for their endless love and support. Thanks for not letting me forget who I am.

Thanks to my “other” family, Diane and Michäel for their patience, support and encouragement.

Finally, I would like to thank all my friends, especially Sandra, Arthur and Sergio for all their support, patience, company and encouragement. Thanks for not letting me give up.

RÉSUMÉ

Les réseaux de capteurs sans fil sont une technologie émergente pour la surveillance de l'environnement. Un réseau de capteurs typique se compose d'un grand nombre de capteurs miniatures (nœuds) multifonctionnels, à faible coût et à faible consommation d'énergie, équipés d'un radio émetteur-récepteur et d'un ensemble de transducteurs pour récolter et transmettre des données environnementales d'une manière autonome.

Une des contraintes les plus importantes de capteurs est la nécessitée d'économiser de l'énergie puisqu'ils utilisent des batteries de duré limitée, généralement irremplaçables. En outre, ils se caractérisent également par une faible vitesse de traitement, capacité de stockage et de bande passante, qui nécessite une gestion des ressources très attentive.

En raison des limitations et caractéristiques inhérentes aux capteurs, le routage dans les réseaux de capteurs sans fil suppose un vrai défi. La tâche de trouver et de maintenir des routes n'est pas triviale étant donné les restrictions d'énergie et les changements soudains dans l'état des nœuds (exemple: mal-fonctionnement) qui entrainent des changements fréquents et imprévisibles dans la structure topologique.

Ce travail présente LBRA, un nouveau protocole de routage géolocalisé qui utilise des antennes intelligentes pour estimer les positions des nœuds dans le réseau, et qui base les décisions de routage sur l'état de connexion des voisins et leur position relative.

L'objectif principal de LBRA est d'éliminer le trafic de contrôle du réseau autant que possible. Pour atteindre cet objectif, l'algorithme emploie la position locale pour prendre des décisions de routage, met en œuvre un nouveau mécanisme pour recueillir les informations de localisation et utilise seulement les nœuds impliqués dans la route pour faire la synchronisation des données de positionnement. De plus, le protocole considère le niveau de la batterie au moment de prendre des décisions de routage afin de balancer la dépense d'énergie du réseau.

LBRA est une version améliorée du routage de ZigBee (norme actuelle pour les réseaux à faible coût et à faible consommation d'énergie) qui se base, lui aussi, sur AODV.

Afin d'évaluer dans quelle mesure LBRA représente vraiment une amélioration par rapport au routage de ZigBee, une série de simulations a été effectué à l'aide du logiciel Network Simulator (ns). Les deux protocoles ont été implantés dans le simulateur. Les performances ont été

comparées dans une variété de scenarios, dans des conditions différentes tels que les charges de trafic, les tailles de réseau et les conditions de mobilité.

Les résultats des expériences ont montré que LBRA réussi à réduire le trafic de contrôle et la charge de routage, tout en améliorant le taux de livraison des paquets, à la fois pour les réseaux fixes et les réseaux mobiles. L'abaissement de l'alimentation du réseau est aussi plus équilibré, puisque les décisions de routage sont prises en fonction du niveau de la batterie des nœuds.

ABSTRACT

Wireless sensor networks are an emerging technology for environmental monitoring. A typical sensor network is composed of a large number of low-cost, low-power, multi-functional miniature sensor devices (nodes) equipped with a radio transceiver and a set of transducers utilized to acquire information about the surrounding environment.

One of the most important constraints of sensor nodes is the low power consumption requirement since they carry limited, generally irreplaceable, batteries. In addition, they are also characterized by scarce processing speed, storage capacity and communication bandwidth, thus requiring careful resource management.

Due to the inherent characteristics and restrictions of sensor nodes, routing in WSNs is very challenging. The task of finding and maintaining routes is nontrivial since energy restrictions and sudden changes in node status (e.g. failure) cause frequent and unpredictable topological changes.

This work introduces a novel location routing protocol that uses smart antennas to estimate nodes positions into the network and to deliver information basing routing decisions on neighbour's status connection and relative position, named LBRA.

The main purpose of LBRA is to eliminate network control overhead as much as possible. To achieve this goal, the algorithm employs local position for route decision, implements a novel mechanism to collect the location information and involves only route participants in the synchronization of location information. In addition, the protocol uses node battery information to make power aware routing decisions.

LBRA is an enhanced version of the ZigBee routing, which is the current standard for reliable, cost-effective and low power wireless networking, and like the latter is prototyped from AODV.

In order to asses to what extent LBRA truly represents an improvement with respect to the ZigBee routing, a series of simulations were designed with the help of the *Network Simulator (ns)*. Basically, both protocols were implemented in the simulator and its performance was compared in a variety of traffic load, network size and mobility conditions.

The experiment results showed that LBRA succeed in reducing the control overhead and the routing load, improving the packet delivery rate for both static and mobile networks. Additionally, network power depletion is more balanced, since routing decisions are made depending on nodes' battery level.

CONDENSÉ EN FRANÇAIS

Les réseaux de capteurs sans fil sont une technologie émergente à faible coût pour la surveillance non-gardée d'un large éventail d'environnements. Ces types de réseaux devrait avoir un impact majeur dans multiple domaines telles que la surveillance, des diagnostics médicaux, le suivi d'objets, surveillance de l'environnement, etc.

Un réseau de capteurs sans fil (RCSF) typique se compose d'un grand nombre de capteurs miniatures (nœuds) multifonctionnels, à faible coût et à faible consommation d'énergie, équipés d'un radio émetteur-récepteur et d'un ensemble de transducteurs pour récolter et transmettre des données environnementales d'une manière autonome.

Un nœud capteur comporte quatre composantes principales: une unité de détection, une unité de traitement, un émetteur-récepteur et une unité d'énergie. Selon l'application et l'objectif spécifique du réseau, le capteur peut nécessiter d'autres composantes telles qu'un système de localisation, un générateur d'énergie, et un dispositif pour le faire bouger. Ces capteurs densément dispersés à l'intérieur d'un phénomène ou très près de lui, ont la capacité de détecter et de réagir aux événements qui se produisent dans leur voisinage [1-3].

Lorsqu'ils sont déployés en grande quantité et en réseau dans un environnement sans fil, ces capteurs peuvent automatiquement s'organiser en réseau ad hoc pour communiquer les uns avec les autres et avec un ou plusieurs nœud-puits (point de collecte) afin de fournir un résultat global de leur fonctionnalité de détection.

Applications des réseaux de capteurs sans fil

Les réseaux de capteurs peuvent être constitués de nombreux types de capteurs tels que sismique, de faible taux d'échantillonnage magnétique, thermique, visuel, infrarouge, acoustique, et les radars, qui sont en mesure de contrôler un large assortiment de conditions ambiantes. Les domaines d'application de cette technologie sont multiples. Par exemple [2] :

- Le domaine militaire

  - Surveillance des forces, de l'équipement et des munitions
  - Surveillance des champs de bataille
- L’environnement
  - Détection des feux de forêt
  - Détection d’inondations [12]
- Le domaine de la santé
  - Administration de médicaments dans les hôpitaux
  - Télésurveillance de données physiologiques [13]
- Le domaine résidentiel
  - Domotique [15]
  - Environnement intelligent [16]
- Le domaine commercial
  - Musées interactifs [17]
  - Détection et suivi de vols de voitures [18]
  - Contrôle environnemental des immeubles à bureaux [17]

Une des contraintes les plus importantes de capteurs est la nécessitée d’économiser de l’énergie puisqu’ils utilisent des batteries de duré limitée, généralement irremplaçables. En outre, ils se caractérisent également par une faible vitesse de traitement, capacité de stockage et de bande passante, qui nécessite une gestion des ressources très attentive.

En raison des limitations et caractéristiques inhérentes aux capteurs, le routage dans les réseaux de capteurs sans fil suppose un vrai défi. La tâche de trouver et de maintenir des routes n'est pas triviale étant donné les restrictions d'énergie et les changements soudains dans l'état des nœuds (exemple: mal-fonctionnement) qui entrainent des changements fréquents et imprévisibles dans la structure topologique.

Ce travail présente LBRA, un nouveau protocole de routage géolocalisé qui utilise des antennes intelligentes pour estimer les positions des nœuds dans le réseau, et qui base ses décisions de routage sur l’état de connexion des voisins et leur position relative.

Définitions et concepts de base

En plus des caractéristiques particulières des capteurs tels que les sources d'énergie irremplaçables et des limitations en vitesse de traitement, capacité de stockage et de bande passante, d'autres facteurs affectent aussi le processus de routage. Parmi eux, on trouve [1,3,4]:

1. *La consommation d'énergie* : extrêmement importante, car la durée de capteur dépend fortement de la durée de batterie, ce qui rend critique le développement de formes de communication qui assurent des économies d'énergie.

2. *Déploiement des Nœuds* : peut être manuel (où les nœuds sont placés un par un) ou aléatoire (où les nœuds sont jetés en masse) en fonction de la demande.
3. *La tolérance de panne* : puisque les nœuds sont sujets à mal fonctionner et ces pannes ne devraient pas affecter la tâche globale du réseau de capteurs.
4. *Modèle de gestion des données* : fait référence à la façon dont les données son livrées aux puits. Ce modèle dépend de l'application et a un impact majeur sur le processus de routage (particulièrement en ce qui concerne l'utilisation optimale de l'énergie et la stabilité des routes), car il détermine le flux de données.
5. *Agrégation des données* : qui est la combinaison de données provenant de différentes sources pour en quelque sorte alléger la redondance.
6. *Extensibilité* : puisque le nombre de nœuds déployés dans la zone de détection peut être de l'ordre de centaines, de milliers, ou plus, et des algorithmes de routage doivent être en mesure de faire face à cette situation.

Le routage dans les réseaux de capteurs se classe généralement en : « *centré sur les données »,* « *hiérarchique »* ou « *basé sur la localisation »*. En plus, selon la façon dont la source trouve la destination, les protocoles de routage peuvent être classés en « *proactive »* dans laquelle les routes sont établies à l'avance, « *réactive* » dans laquelle les routes sont établies à la demande ou « *hybride* » qui combine les deux autres.

Dans le routage *centré sur les données*, le puits envoie des requêtes à certaines régions et attend les données provenant de capteurs situés dans ces régions. Dans ce genre de réseaux chaque nœud joue généralement le même rôle et les capteurs collaborent pour accomplir la tâche de détection.

Dans le routage *hiérarchique*, s'effectue une division du réseau en plusieurs sous-ensembles ou régions. L'objectif principal de ce type de routage est de maintenir efficacement la consommation d'énergie par l'agrégation des données afin de diminuer le nombre des messages transmis. Dans chacune de ces régions la transmission de paquets est effectuée par le biais d'un système de coordonnées locales et la communication entre les régions est effectuée pour diriger les données vers le nœud-puits. Dans cette approche les nœuds jouent des rôles différents dans le réseau.

Dans le routage *basé sur la localisation*, la position des capteurs est exploitée pour acheminer les données dans le réseau. Chaque nœud décide à quel voisin transmettre le message basé uniquement sur son emplacement, celui de ces voisins, et celui de la destination [5]. L'information de la localisation est principalement utilisée pour calculer la distance entre deux nœuds afin d'estimer la consommation d'énergie nécessaire pour la communication.

Aspects du problème

Le routage dans les réseaux de capteurs sans fil est très difficile en raison des caractéristiques particulières qu'ils possèdent et qui les distinguent des réseaux de communication traditionnelles et des réseaux ad hoc. Ces distinctions font que l'utilisation des mécanismes de routage spécialement conçus pour ces types de réseaux n'est pas appropriée. Les principales différences sont [1-4]:

1. Il n'est pas possible de construire un système d'adressage global pour le déploiement d'un grand nombre de capteurs puisque la charge d'entretien des identificateurs est élevée.

   En plus, les protocoles de routage basés sur IP traditionnels font le routage en utilisant l'adresse de destination et l'information stockée dans les tables de routage qui indique

le prochain saut vers cette destination. Cependant, dans les réseaux de capteurs sans fil, où les nœuds peuvent être déployés de manière aléatoire et en grande quantité, et qui ont des variations de topologie fréquentes dues aux pannes ou aux changement dans l'état des nœuds pour économiser de l'énergie, la surcharge des messages nécessaires pour maintenir les tables de routage et l'espace de mémoire requis pour les stocker n'est pas abordable [3].

Par conséquent, les protocoles classiques basés sur IP ne peuvent pas être appliqués aux RCSFs.

2. La plupart des applications de réseaux de capteurs requiert le flux des données captées à partir de sources multiples pour un récepteur unique.
3. Les données générées sont très redondantes étant donné que plusieurs capteurs situés dans la même région peuvent générer des données identiques. Cette redondance doit être exploitée par les protocoles de routage afin d'améliorer l'efficacité énergétique et l'utilisation de bande passante.
4. Les capteurs sont fortement limités en termes de ressources, ce qui nécessite une gestion minutieuse.
5. Les réseaux de capteurs sont spécifiques à l'application (c'est-à-dire : la conception d'un réseau de capteurs dépend de l'application).

Bien que de nombreux algorithmes de routage pour les RCSF aient été proposés à la suite des différentes approches qui existent, dans [6] il a été démontré que les protocoles de routage qui n'utilisent pas des informations de localisation géographique ne sont pas extensibles. En plus, dans [3] il a été établi que les protocoles de routage idéaux pour le RCSF doivent baser les décisions de routage sur les informations échangées entre les nœuds voisins, offrir la fiabilité dans le réseau, et requérir un minimum de trafic de control, consommation d'énergie et encombrement de mémoire. Pour ces raisons, la plupart des recherches sur le routage dans les RCSF sont concentrées sur les protocoles géolocalisés ou basées sur la localisation.

Les algorithmes de routage géolocalisés évitent la surcharge de trafic de contrôle en limitant l'échange de messages au minimum pour connaître la position exacte des voisins et avoir une idée approximative de la position de la destination. Ceci est très pratique pour les réseaux avec des contraintes d'énergie critiques comme les RCSF [5]. En outre, des informations de localisation peuvent également être utilisées pour identifier une source de données selon les besoins de l'application. Nonobstant, l'utilisation de protocoles géolocalisés pose aussi des problèmes évidents en termes de fiabilité. La précision de la position de la destination est un problème important à considérer.

La méthode la plus simple pour résoudre le problème de localisation est d'équiper tous les nœuds d'un récepteur GPS qui permettrait d'assigner des coordonnées réelles aux nœuds dans le réseau. Toutefois, cette solution est coûteuse en raison des coûts du récepteur GPS, la consommation d'énergie et les exigences de format. De plus, la méthode peut échouer si tous les nœuds ne reçoivent pas les signaux GPS.

Une bonne alternative serait d'équiper d'un récepteur GPS (ou fournir manuellement des coordonnées correctes) seulement quelques nœuds, et sur cette base, calculer les coordonnées d'autres nœuds. Néanmoins, bien que cette solution soit moins onéreuse que la première en termes de nombre total de récepteurs GPS nécessaires, elle pourrait être plus coûteuse en termes de trafic de contrôle et de consommation d'énergie, dû à l'échange d'informations nécessaires pour calculer les coordonnées d'autres nœuds. Il pourrait aussi y avoir des erreurs importantes de mesure et d'approximation.

Une autre solution consiste à assigner des coordonnées virtuelles aux nœuds en fonction de la connectivité du réseau; les coordonnées relatives des nœuds voisins sont obtenues en échangeant ces informations entre voisins.

Le principal inconvénient de cette solution est que cela entraîne une complexité importante des calculs et une surcharge des messages (inondations). De plus, elle requiert un espace de mémoire dans le nœud, déjà fortement limitée.

Une nouvelle approche, qui est restée inexplorée jusqu'à tout récemment, est l'utilisation d'antennes intelligentes. Elles permettent l'estimation précise des positions des nœuds,

améliorent la communication dans le réseau en diminuant la consommation d'énergie et, par conséquent, augmentent sa durée de vie.

Une antenne intelligente est une antenne composée de nombreux éléments d'antenne qui sont disposées de façon linéaire, circulaire ou planar. Leur rôle est d'augmenter la qualité du signal radio par l'optimisation de la propagation radioélectrique et accroître la capacité du medium en augmentant l'utilisation de bande passante. Leur intelligence réside dans la combinaison des signaux reçus dans les éléments d'antennes intelligentes [7].

Les antennes intelligentes ont été longtemps considérées comme inappropriées pour les RCSF à cause de leur volume plus grand que les antennes traditionnelles dû au plus grand nombre d'éléments d'antenne. Le traitement de plus d'un signal nécessite, également une plus grande puissance de calcul et une électronique capable de traduire la fréquence radio (RF) en une bande de base appropriés.

Toutefois, il a été démontré expérimentalement que l'utilisation des antennes intelligentes peut augmenter la capacité globale du réseau et réduire considérablement la consommation d'énergie. En outre, il a été démontré que l'utilisation des antennes intelligentes dans les réseaux de capteur est obligatoire dans certains cas, et possible dans d'autres, pour un coût supplémentaire minimal [7-10].

LBRA (The location based routing algorithm)

L'objectif principal de LBRA est d'éliminer le trafic de contrôle du réseau autant que possible. Pour atteindre cet objectif, l'algorithme emploie la position locale pour prendre des décisions de routage, met en œuvre un nouveau mécanisme pour recueillir les informations de localisation et utilise seulement les nœuds impliqués dans la route pour faire la synchronisation des données de positionnement. De plus, le protocole considère le niveau de la batterie au moment de prendre des décisions de routage afin d'équilibrer la dépense d'énergie du réseau.

LBRA est une version améliorée du routage de ZigBee (norme actuelle pour les réseaux à faible coût et à faible consommation d'énergie) qui se base, lui aussi, sur AODV.

LBRA est composée de trois étapes:

1. *Découverte de la route (RD)*, dans lequel les nœuds cherchent des routes pour communiquer entre eux.
2. *Établissement de la route (RE)*, dans lequel les nœuds établissent des connexions dans les deux sens par l'échange des informations requises
3. *Maintenance de la route (RM)*, qui constitue un mécanisme pour sélectionner la meilleure route en termes de consommation d'énergie parmi les routes trouvés pendant la phase de découverte.

La découverte de la route, à son tour est divisée en deux étapes:

1. Route-demande (RREQ), dans lequel un nœud source cherche un nœud destination spécifique dans le réseau.
2. Route-réponse (RREP) qui permet la mise en place de la route de communication bidirectionnelle entre les nœuds, une fois que le nœud de destination est trouvé.

En LBRA il y a deux scénarios possibles pour le processus de RD: l'inondation et l'inondation limitée. Le choix du scénario dépendra de la connaissance de la position du nœud de destination: si le nœud source connaît l'emplacement du nœud de destination, il utilise l'inondation limitée, sinon, il inonde l'ensemble du réseau.

Le processus de découverte de la route se fait soit lorsque le nœud source ne connaît pas de route pour atteindre le nœud de destination, ou si une route préalablement établi entre eux n'est plus disponible. Dans cette dernière situation, puisque les nœuds ont déjà communiqué, les emplacements de chaque nœud est disponible et au lieu d'inonder l'ensemble du réseau à la recherche d'une route, LBRA passera au scénario d'inondation limitée en la restreignant à une zone spécifique, appelé la zone cible.

En LBRA, en plus d'établir des connexions entre les nœuds, les inondations servent également à synchroniser les informations de localisation dans le réseau et à calculer le coût de relai, qui correspond à la somme du coût d'utilisation des nœuds appartenant à la route qui est explorée.

Lorsqu'un processus de découverte de route est déclenché, le nœud source peut recevoir de nombreux messages de réponse (RREP), chacun avec une route différente vers le nœud

de destination. En général, l'ordre d'arrivée de ces messages ne dépend que du nombre de nœuds qui composent la route: moins il y aura de nœuds dans la route, plus la réponse atteindra la destination rapidement. Toutefois, en termes de consommation d'énergie, la meilleure route ne sera pas nécessairement celle qui a le moins de nœuds.

En LBRA, cette situation est traitée par l'acceptation subséquente de messages de réponse et le remplacement de la route, si le coût de la transmission de la nouvelle est moins élevé. Pourtant, le nœud source commencera la transmission de données dès que la première route sera découverte sans tenir compte qu'elle soit optimale en termes d'énergie ou non.

Afin d'évaluer dans quelle mesure LBRA représente vraiment une amélioration par rapport au routage de ZigBee, une série de simulations a été effectué à l'aide du logiciel Network Simulator (ns). Les deux protocoles ont été implantés dans le simulateur. Les performances ont été comparées dans une variété de scenarios, dans des conditions différentes tels que les charges de trafic, les tailles de réseau et les conditions de mobilité (réseaux mobiles et statiques).

Les expériences ont été réalisées avec les nœuds statiques et en mouvement, avec les nœuds se déplaçant à différentes vitesses et avec des topologies différentes. Pour chacune des expériences, quatre scénarios ont été utilisés, avec plusieurs charges de trafic: faible, moyenne, normale et haute.

Les résultats des expériences ont montré que LBRA réussi à réduire le trafic de contrôle et la charge de routage, tout en améliorant le taux de livraison des paquets, à la fois pour les réseaux fixes et les réseaux mobiles. L'abaissement de l'alimentation du réseau est aussi plus équilibré, puisque les décisions de routage sont prises en fonction du niveau de la batterie des nœuds.

INDEX

INDEX OF TABLES

INDEX OF FIGURES

LIST OF ACRONYSMS AND ABREVIATIONS

AOA	Angel of Arrival
AODV	Ad hoc On Demand Distance Vector
CONSER	Collaborative Simulation for Education and Research
DARPA	Defense Advanced Research Projects Agency
DID	Destination Node Identifier
DSR	Dynamic Source Routing protocol
ESPRIT	Estimation of Signal Parameters via Rotational Invariance Techniques
GPS	Global Positioning System
ICIR	ICSI Center for Internet Research
ICSI	International Computer Science Institute
IP	Internet Protocol
LBL	Lawrence Berkeley National Laboratory
MAC	Medium Access Control
MN	Mobile Node
MUSIC	Multiple Signal Identification and Classification
MVDR	Minimum Variance Distortionless Response
NS	Network Simulator
NSF	National Science Foundation
PAN	Personal Area Network
PARC	Palo Alto Research Center
PHY	Physical
QoS	Quality of Service
RD	Route Discovery
RDT	Route Discovery Table
RE	Route Establishment
RF	Radio Frequency
RM	Route Maintenance
RREP	Route Reply
RREQ	Route Request

RREQID	Route Request Identifier
RSSI	Received Signal Strength Indicator
RT	Routing Table
SAMAN	Simulation Augmented by Measurement and Analysis for Networks
SID	Source Node Identifier
SNR	Signal Noise Ratio
Tcl	Tool command language
TCP	Transmission Control Protocol
TDOA	Time Difference of Arrival
TOA	Time of Arrival
UCB	University of California in Berkeley
UDP	User Datagram Protocol
USC/ISI	The Information science institute of the Universiti of southern California
VINT	Virtual Inter Network Testbed
WSN	Wireless Sensor Network
ZC	ZigBee Coordinator
ZED	ZigBee End Device
ZR	ZigBee Router

CHAPTER 1 INTRODUCTION

Wireless Sensor Networks (WSNs) are an emerging technology for low cost, unattended monitoring of a wide range of environments. These kinds of networks are expected to have major impact on multiple application scenarios such as surveillance, environmental monitoring, medical diagnosis, object tracking, etc.

A WSN is composed of a sheer number of sensors nodes capable of observing and reacting to changes in ambient conditions in the environment surrounding them and then transforming these measurements into signals that can be processed. When networked together these sensor nodes, fitted up with transceivers to communicate either among each other or directly to an external base station (sink), coordinate among themselves to produce high-quality information about the physical environment. Each sensor node bases its decisions on its mission, the information it currently has and its knowledge of its computing, communication, and energy resources [1-3].

One of the most important constraints of sensor nodes is the low power consumption requirement since they carry limited, generally irreplaceable, batteries. In addition, they are also characterized by scarce processing speed, storage capacity and communication bandwidth, thus requiring careful resource management.

Due to the inherent characteristics and restrictions of sensor nodes, routing in WSNs is very challenging. The task of finding and maintaining routes is nontrivial since energy restrictions and sudden changes in node status (e.g. failure) cause frequent and unpredictable topological changes [1].

This work presents a novel location routing protocol based on smart antennas for wireless sensor networks. This introductory chapter presents the basic concepts of WSNs and the elements of the problem, followed by our research's objectives and finally the outline.

1.1 Definitions and basic concepts

Besides the special characteristics of sensor nodes such as irreplaceable power sources and limited processing speed, storage capacity and communication bandwidth, other factors also affect the routing process. Among them we found: *energy consumption*, extremely important since sensor node lifetime has a strong dependence on battery duration making critical the development of energy-conserving communication forms. N*ode deployment* that can be manual (where nodes are place one by one) or randomized (where nodes are thrown in mass) depending

on the application. *Fault tolerance* since nodes are prone to failure and these failures should not affect the overall task of the sensor network. The *data delivery model* to the sink which is also application dependant and has great impact on the routing process (especially with regard to the optimal use of energy and route stability) since it determines the flow of data. The *data aggregation / fusion* which is the combination of data from different sources to somehow lighten redundancy, and the *scalability* since the number of sensor nodes deployed in the sensing area may be on the order of hundreds or thousands, or more, and routing algorithms must be able to cope with that [1, 3, 4].

Routing in WSNs can be generally categorized into *data-centric*, *hierarchical* and *location-based*. Besides, depending on how the source finds the destination, routing protocols can be classified into *proactive* in which routes are computed before they are needed, *reactive* in which routes are computed on demand or *hybrid* that combines the other two.

In the *data-centric* routing, the sink sends queries to certain regions and waits for data from sensors located in those regions. In this kind of networks each node typically plays the same role and sensor nodes collaborate to perform the sensing task. In the *hierarchical* routing, nodes play different roles in the network. This approach divides the network into a set of regular linked regions where intra-region packet forwarding is performed by the means of a local coordinate system defined within each region (where is also carried out data aggregation and fusion) and inter-region forwarding is performed to direct data to the sink. In *location-based* routing, sensor nodes' positions are exploited to route data in the network. Each node makes a decision to which neighbour to forward the message based solely on the location of itself, its neighbouring nodes, and the destination [5]. Location information is mostly used to calculate the distance between two particular nodes so that routing energy consumption required for communication can be estimated.

1.2 Aspects of the problem

Routing in WSNs is very challenging due to the inherent characteristics that distinguish them from contemporary communication networks or wireless ad hoc networks making unsuitable the use of routing techniques especially designed for these latter.

First of all, it is not possible to build a global addressing scheme for the deployment of large number of sensor nodes as the overhead of ID maintenance is high. Furthermore, traditional IP-based routing protocols impose a hierarchical addressing structure on the network and base

routing decisions (i.e. packet forwarding) on the destination address and a set of tables indicating the next hop to reach that address. In WSNs, where nodes can be deployed at random and in large quantities and with frequent topology variations due to sensor failures or energy efficiency decisions, the message overhead to maintain the routing tables and the memory space required to store them is not affordable [3]. Hence, classical IP-based protocols cannot be applied to WSNs.

Second, in contrast to typical communication networks, almost all applications of sensor networks require the flow of sensed data from multiple sources to a particular sink. Third, generated data traffic has significant redundancy since data collected by nodes located in the same vicinity is typically based on common phenomena. Such redundancy must be exploited by the routing protocols to improve energy and bandwidth utilization. Fourth, sensor nodes are tightly constrained in terms of energy, processing and storage capacities, thus requiring cautious resource management. Fifth, position awareness of sensor nodes is important since data collection is normally based on location. Finally, sensor networks are application-specific (i.e., design requirements of a sensor network change with application) [1-4].

Although many routing algorithms for WSNs have been proposed following the different approaches cited in section 1.1, in [6] has been shown that routing protocols that do not use geographical location information are not scalable and in [3] is set that ideal routing protocols for WSNs should base routing decisions on information exchanged with neighbours, offer network reliability and require minimal message overhead, power consumption and memory footprint. For these reasons most of the research on routing in WSNs has focused on localized or position-based protocols.

Localized routing algorithms avoid control-traffic overhead by requiring only accurate neighbourhood information and a rough idea of the position of the destination which is extremely suitable for networks with critical power-constrained resources at nodes such as WSNs [5]. Besides, location information can also be used to identify a data source for application requirements; however, the use of localized protocols poses evident problems in terms of reliability. The accuracy of the destination's position is an important problem to consider.

The simplest method to resolve the location problem is to provide all nodes with a GPS receiver that would allow assigning real coordinates to nodes into the network. However, this is an expensive solution due to GPS receiver's cost, power consumption and size requirements. In addition, it may also fail to work if some nodes cannot receive GPS signals. A better solution

could be to provide with a GPS receiver (or manually provide correct coordinates) only a few anchor nodes, and based on these, calculate other nodes' coordinates. Nonetheless, although this solution is cheaper than the former in terms of the total number of GPS receivers required, it could be costlier in terms of message overhead and power consumption due to the information exchange required for approximating the coordinates of non-anchors nodes. Furthermore, it might suffer from important measurement and approximation errors.

An alternative solution is to assign virtual coordinates to nodes based on network connectivity; relative coordinates of neighbouring nodes can be obtained by exchanging such information between neighbours. The main drawback of this solution is that entails important computational complexity and message (floods) overhead and also requires per-node memory space, a scarce resource itself.

A novel approach, that remained until recently unexplored, is the use smart antennas to estimate nodes positions accurately and to improve network communication, decreasing power consumption and therefore increasing its lifecycle.

A smart antenna is an antenna composed of many antenna elements that are arranged in a linear, circular or planar configuration. Their role is to increase the radio signal quality by optimizing radio propagation and to increase medium capacity by increasing bandwidth utilization. Their smartness resides in the combination of the signals received within the smart antenna elements [7].

Smart antennas in general have been for long considered unsuitable for integration in wireless sensor nodes. They consist of more than one antenna element and therefore require a larger amount of space than traditional antennas. In addition to that, the processing of more than one signal requires more computational power and electronics capable of translating radio frequency (RF) signals to baseband signals suitable processing. However, it has been experimentally demonstrated that the use of smart antennas can increase overall network capacity and significantly reduce power consumption. Moreover, it has been shown that the use of smart antennas in sensor networks is in some cases obligatory and in other cases achievable, with minimal additional cost [7-10] .

This work introduces a novel location routing protocol that uses smart antennas to estimate nodes positions into the network and to deliver information basing routing decisions on neighbour's status connection and relative position.

1.3 Research goals

The main goal of our research is to propose a novel location-based routing protocol for wireless sensor networks that uses smart antennas to improve overall routing performance. By using smart antennas, the direction of received signal and the distance between sensor nodes can be estimated. More specifically, the goals are the following:

- To analyze the existing location routing solutions for WSNs.
- To propose an energy-efficient location routing protocol based on smart antennas for WSNs.
- To evaluate the performance of the proposed algorithm(s) by means of simulations, comparing them to the current solutions in order to measure the contribution of this work.

1.4 Outline

The rest of the report is organized as follows. Chapter 2 presents the background regarding wireless sensor networks and the different location routing strategies proposed. Chapter 3 introduces the proposed location-based protocol. Chapter 4 shows the algorithm's implementation in a network simulator and the results obtained. At last we conclude in Chapter 5 with final remarks and future work.

CHAPTER 2 ROUTING IN WIRELESS SENSOR NETWORKS

Wireless sensor networks are an emerging technology for environmental monitoring. A typical sensor network is composed of a large number of low-cost, low-power, multi-functional miniature sensor devices (nodes) equipped with a radio transceiver and a set of transducers utilized to acquire information about the surrounding environment.

A sensor node has four main components: a *sensing unit*, a *processing unit*, a *transceiver unit* and a *power unit*. Additionally, depending on the application and the specific purpose of the network, sensor devices may require other components such as a location system, a power generator, and a mobilizer. These sensor nodes densely scattered either inside a phenomenon or very close to it, have the capability to sense and to react to events happening in their vicinity.

When deployed in large quantities and networked together over a wireless medium, these sensors can automatically organize themselves into an ad hoc multihop network to communicate with each other and with one or more sink (command center) nodes in order to provide an overall result of their sensing functionality.

2.1 Sensor networks applications

Sensor networks may consist of many different types of sensors such as seismic, low sampling rate magnetic, thermal, visual, infrared, acoustic, and radar, which are able to monitor a broad assortment of ambient conditions. Networking unattended sensor nodes are expected to have major impact in a wide variety of domains such as [2]:

- Military
  - monitoring forces, equipment and ammunition
  - battlefield surveillance
  - reconnaissance of opposing forces and terrain
  - targeting
  - battle damage estimation
  - nuclear, biological and chemical attack detection and reconnaissance
- Environment
  - forest fire detection
  - biocomplexity mapping of the environment [11]

- flood detection [12]
- precision agriculture

- Health
  - telemonitoring of human physiological data [13]
  - tracking and monitoring doctors and patients inside a hospital
  - drug administration in hospitals [14]
- Home
  - home automation [15]
  - smart environment [16]
- Other commercial areas
  - environmental control in office buildings [17]
  - interactive museums [17]
  - detecting and monitoring car thefts [18]
  - managing inventory control
  - vehicle tracking and detection [19]

2.2 Types of sensor networks

There are five types of sensor networks [20]:

1. *Terrestrial WSNs* [2], typically composed of hundreds to thousands of inexpensive wireless sensor nodes deployed in a given area.
2. *Underground WSNs* [21], which consist of a number of sensor nodes buried underground or in a cave or mine used to monitor underground conditions. This kind of network is more expensive than a terrestrial WSN in terms of equipment, deployment, and maintenance. Underground sensor nodes are expensive because appropriate equipment parts must be selected to ensure reliable communication through soil, rocks, water, and other mineral contents.
3. *Underwater WSNs* [22], which consist of a number of sensor nodes and vehicles deployed underwater. As opposite to terrestrial WSNs, underwater sensor nodes are more expensive and fewer sensor nodes are deployed. Autonomous underwater vehicles are used for exploration or gathering data from sensor nodes. Typical underwater wireless communications are established through transmission of acoustic waves.

4. *Multi-media WSNs* [23], which consist of a number of low cost sensor nodes equipped with cameras and microphones. These kinds of networks have been proposed to enable monitoring and tracking of events in the form of multi-media such as video, audio, and imaging.
5. *Mobile WSNs*, which consist of a collection of sensor nodes that can move on their own and interact with the physical environment. Mobile nodes have the ability to sense, compute, and communicate like static nodes. A key difference is mobile nodes have the ability to reposition and organize itself in the network. A mobile WSN can start off with some initial deployment and nodes can then spread out to gather information. Information gathered by a mobile node can be communicated to another mobile node when they are within range of each other.

2.3 WSNs architecture

Hundreds or thousands of sensor nodes are scattered in a sensor field as shown in Figure 2.1.

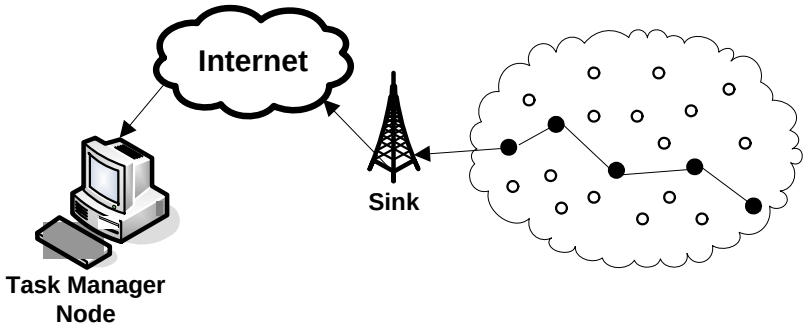


Figure 2.1: Sensor network topology

2.3.1 Protocol stack

The protocol stack, illustrated in Figure 2.2, consists of:

1. *Application layer*: remains a vastly unexplored area for sensor networks. Depending on the sensing tasks, diverse types of application SW can be used on this layer. Three possible application protocols are [2]:

    a. The *sensor management protocol* (SMP), which allows system administrators to interact with sensor networks and perform administrative tasks such as time synchronization of the nodes, movement of nodes, turning on or turning off the radio transceivers of nodes, etc.

b. The *task assignment and data advertisement protocol* (TADAP), which allows interest dissemination in two ways: either the users send their interest about a certain attribute of the phenomenon or a triggering event to the network or to a subset of nodes, or the nodes advertise the available data to the users and the users query the data in which they are interested.

c. The s*ensor query and data dissemination approach* (SQDDP), which provides user applications with interfaces to issue queries, respond to queries and collect incoming replies.

2. *Transport layer*: especially needed when the system is planned to be accessed from the Internet or any other external network. A possible approach is the TCP splitting [24] in which the communication between the user and the sink node is by UDP or TCP via Internet and the communication between the sink and sensor nodes may be purely UDP since sensor nodes have limited memory.

3. *Network layer*: requires special multihop wireless routing protocols between the sensor node and the sink. This layer is usually designed according to the following principles [2]: power efficiency is always important, sensor networks are mostly data centric, data aggregation should not affect the collaborative effort of the nodes and attribute based addressing and location awareness are ideal. Special factors and considerations regarding the network layer are studied in more detail in section 2.3.

4. *Data link layer*: ensures point-to-point and point-to-multipoint connection in a communication network and is in charge of the creation of the network infrastructure and the fairly and efficient coordination of communication resources among sensor nodes. MAC protocols for sensor networks must have built-in power conservation, mobility management and failure recovery.

5. *Physical layer*: responsible for frequency selection, carrier frequency generation, signal detection, modulation and data encryption in a power efficient way. The most important factor when designing sensor networks is power conservation.

6. *Management planes*: used to allow sensor nodes to collaborate among them in a power efficient way (prolonging sensor network lifetime), to route data into the network and to share resources. Without them, each sensor node will work independently.

- The *power management plane* manages how a node utilizes its power. For example, the node, to avoid duplicated messages, may turn off its transceiver device after receiving a message from a neighbour. Also, when the power is low, may broadcast to its neighbours that its power is low and cannot serve as relay.
- The *mobility management plane* identifies and records sensor nodes movements maintaining routes and keeping track of neighbour nodes. By knowing its neighbours, sensor nodes can balance their power and task usage [2].
- The *task management plane* balances and schedules the sensing tasks given to a specific region. For example, special nodes located in that region, chosen depending on its power level or particular sensing capabilities, might be required to sense the environment while the others must be inactive.

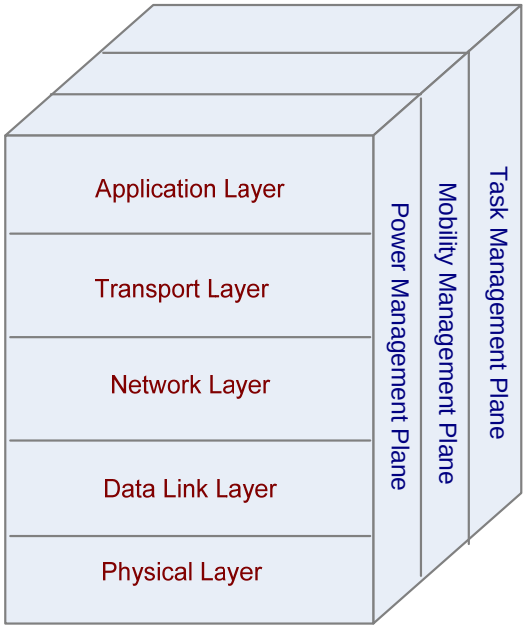


Figure 2.2: The sensor network protocol Stack

2.4 Design issues

Despite the wide assortment of domains in which WSNs are applicable, these networks have important restrictions such as low power consumption requirement, since sensor nodes carry limited and generally irreplaceable batteries, limited processing speed, limited storage capacity and limited communication bandwidth, thus requiring careful resource management.

Given that the performance of a routing protocol is closely related to the architectural model, this section summarizes several factors and design issues that affect the routing process.

2.4.1 Energy consumption

Energy efficiency is one of the most important issues in WSNs due to the power constraints imposed by the size of nodes. In fact, sensor node lifetime has a strong dependence on battery duration which makes crucial the development of procedures that extend battery lifetime as much as possible.

The main task of a sensor node in a sensor field is to detect events, perform quick local data processing, and then transmit the data. Hence, power consumption can be divided into three domains: *sensing*, *communication*, and *data processing*, being the communication domain the greatest power consumer [2]. The radio transceiver with transmission and reception operations having similar energy requirements is the most voracious device on a sensor node in terms of energy demands.

The major reason for energy waste is *idle listening*, where a node is listening to the radio channel, waiting for something. Other reasons include packet collisions, overhearing a packet destined to another node and control packet overhead [25].

2.4.2 Data management model

Sensor networks are created to provide users with relevant information from the chosen sensor field. Depending on the application of the sensor network, the data delivery model to the sink can be *continuous*, *event-driven*, *query-driven* and *hybrid* [26].

The *continuous* model, in which every node sends data to the sink at regular intervals, is suitable for applications that require periodic data checking such as monitoring the level of air pollution in real time. In the *event-driven* model, well suited to time critical applications such as fire forest detection, each node periodically checks if certain environmental conditions are satisfied or match a predefined pattern, stores event data and sends it to the sink. In the *query-driven* model, also suitable for time critical applications, the transmission of data is triggered when a query is generated by the sink. An example of use could be requesting to nodes located in areas where the temperature is over 70°F to measure the pressure. The *hybrid* model is a combination of the others.

The routing protocol is highly influenced by the data management model, especially with regard to the optimal use of energy and route stability [1].

2.4.3 Node deployment

Node deployment in WSNs is application dependent and can be either deterministic or self-organizing: in deterministic situations, the sensors are manually placed and data is routed through pre-determined paths; in self organizing systems, nodes are randomly deployed creating an ad hoc routing infrastructure [4].

In [2] node deployment is divided in three phases: the *pre-deployment and deployment phase* in which sensor nodes can be either thrown in mass or manually placed one by one in the sensor field, the *post-deployment phase*, during which sensor networks may present significant topological variations due to changes in nodes (malfunctioning, reachability, task details, power availability, mobility, etc.) and the *re-deployment phase* in which additional sensors may be deployed in order to replace the malfunctioning nodes or due to changes in task dynamics.

2.4.4 Data aggregation/fusion

Data aggregation is the combination of data from different sources. The use of this technique in WSNs is very convenient for two main reasons: similar packets from multiple sources can be aggregated reducing redundancy and therefore the number of transmissions, and knowing that data processing would be less energy consuming than communications [27], substantial energy savings can be achieved.

2.4.5 Scalability

The number of sensor nodes in a sensor field may be on the order of hundreds, thousands or even millions. Any routing scheme must be able to work with this huge number of nodes.

2.4.6 Fault tolerance

Sensor nodes are prone to fail due to lack of power, physical damage, or environmental interference. The failure of single nodes should not affect the overall task of the sensor network.

2.4.7 Localization

The goal of localization is to supply location information for nodes in a sensor network. This information can be used by routing algorithms and or by applications in order to identify data source location or to issue queries.

Most of the routing protocols for sensor networks require location information for sensor nodes in order to calculate the distance between two particular nodes so that the energy consumption needed for communication can be estimated. Since localization is a key piece of our research, this aspect will be tackled in detail in chapter 3.

2.5 Routing challenges in WSNs

Routing in sensor networks is very challenging due to several characteristics that distinguish them from traditional communication and ad hoc networks. Main differences are [4] [1]:

1. It is not possible to build a global addressing scheme for the deployment of sheer number of sensor nodes (the number of sensor nodes on a sensor network can reach millions).
2. Most applications of sensor networks require the flow of sensed data from multiple sources to a single sink.
3. Generated data traffic has significant redundancy in it since multiple sensors located in the same area may generate identical data.
4. Sensor nodes are tightly constrained in terms of transmission power, on-board energy, processing capacity and storage, thus requiring careful resource management.
5. Sensor networks are application-specific

IP-based routing protocols base routing decisions on routing tables indicating the next hop to reach the destination address. In WSNs, with important energy and memory limitations, and with the possible presence of an enormous quantity of nodes randomly deployed, the message overhead and the memory space required for maintaining and storing the routing tables is not affordable.

Some Ad hoc protocols, adapted for WSNs, such as AODV [28] and DSR[29] somehow lighten these problems but have serious scalability issues due to its dependency on flooding for route discovery [3]. Yet, ZigBee, the current standard defined for wireless sensor networks developed

by the ZigBee Alliance [30] and built upon the IEEE 802.15.4 [31] standard, is based on the Ad hoc On Demand Distance Vector routing algorithm (AODV [28]).

Flooding is a classical reactive technique to relay data in sensor networks without the need for any routing algorithms and topology maintenance. In flooding, a node receiving a packet broadcasts it to its neighbours, unless it is the destination node or a maximum number of hops is reached. This technique has several deficiencies such as [32]: *implosion* (duplicate messages are sent to the same node), *overlap* (neighbour nodes receive duplicated messages) and *resource blindness* due to the lack of attention paid to available energy resources.

Routing in WSNs is generally classified based on network structure as *data-centric*, *hierarchical* or *location based*. However, there are other distinctive categorizations based on network flow or quality of service (QoS) awareness. In addition to that, routing protocols in general are commonly categorized as *proactive*, *reactive* and *hybrid*, depending on how the source finds a route to the destination. Proactive protocols compute routes before they are needed, while reactive protocols compute routes on demand. Hybrid protocols combine these two models.

2.5.1 Data-centric routing

In WSNs, the lack of global identification (due to the sheer number of sensor nodes scattered in the sensor field) along with the random deployment of such nodes makes the generated data transmitted within the network extremely redundant. Since this is very inefficient in terms of energy consumption, routing protocols capable to select a set of sensor nodes and use data aggregation during the relaying of data have been considered [4]. This consideration has led to *data-centric* routing in which all nodes are typically assigned equal roles or functionality.

In *data-centric* routing, the sink sends queries to certain regions and waits for data from the sensors located in the selected regions. Since data is being requested by the means of queries, attribute-based naming is necessary to specify the properties of data. The most representative protocol of this routing paradigm is *directed diffusion.* Many other protocols have been proposed either based on it or following a similar concept.

Directed diffusion [33] is a query-driven protocol in which a request for a precise kind of data is interpreted as an *interest* with a certain data rate (an interest is defined using a list of attribute-value pairs such as name of objects, interval, duration, geographical area, etc). In order to propagate the interest through the network, the sink broadcasts an *interest message* to its neighbors, which before forwarding it to its respective neighbors, record the message and the data

rate and set up a gradient (a reply link) toward the source of the message (the neighbor from which the interest was received). Nodes that detect or receive data matching one of their cached interests forward such data along the gradients with the corresponding data rate. Via neighboring dissemination the data reaches the sink.

The main advantage of *directed diffusion* is that data exchange is exclusively based on locally exchanged interests with no need for a node addressing mechanism. A disadvantage is load unbalance since nodes close to the sink have to manage a large part of control data traffic. Additionally, the possibility of data aggregation is very limited since similar information coming from different sources can be combined only if it is routed through a common node. As a final point, the fact of being query-driven makes directed diffusion not suitable for applications that require another data delivery model.

2.5.2 Hierarchical based routing

The *hierarchical or cluster based* routing approach takes a condensed representation of the global sensor network topology structure, which identifies and divides the network into a set of regular regions, and stores it in every node. A local coordinate system is defined within each region and a greedy-like routing is used to perform intra region packet forwarding. The representation is used to link the regions and make long routing across the network [3].

The aim of *hierarchical or cluster* routing is to efficiently maintain the energy consumption by performing data aggregation and fusion decreasing the number of messages transmitted, to contribute to system scalability by having a two layer routing scheme that allows the system to cope with additional load and to cover a large area of interest without degrading the service and prolonging the network lifespan.

In this approach, nodes will play different roles in the network. Cluster formation is typically based on the energy reserve of sensor and sensor's proximity to the cluster head; higher-energy nodes can be used to process and send the information, while low-energy nodes can be used to perform the sensing in the proximity of the target.

One of the first hierarchical routing protocols proposed for sensor networks is the *Low-energy adaptive clustering hierarchy (LEACH)* protocol [27] that later became a milestone from which many other hierarchical protocols have been derived.

In LEACH the idea is to form clusters of the sensor nodes based on the received signal strength and randomly select cluster heads (CH) rotating this role to evenly distribute the energy load

among the sensors in the network. All the data processing such as data fusion and aggregation are local to the cluster. The CH compresses the data arriving from nodes belonging to its respective cluster and then sends an aggregated packet to the sink. This protocol is especially appropriate for continuous monitoring applications.

The main disadvantage of the *hierarchical approach* may lie on the complexity of deriving the high level topological structure of the whole network. In addition, the size of this representation must suit node memory constraints and local coordinate systems within regions are complex.

2.5.3 Location based routing

In *location-based* routing sensor nodes' positions are exploited to route data in the network and sensor nodes are addressed by means of their position. In this kind of routing location information is used by protocols to calculate the distance between two particular nodes so that energy consumption required for communication can be estimated. To save energy, some location-based schemes demand that nodes go to sleep if there is no activity, having as many sleeping nodes in the network as possible [1]. Localized protocols can be *tree-based* or *geographic-based.*

The *tree-based* model is commonly used in applications involving *environmental observation* where sensor readings are sent to the sink. In this model each node just knows its parent towards the sink and forwards it any message it receives or originates (see Figure 2.3).

Routing trees are easy to construct and maintain, but are not suitable for complex applications that require end-to-end communication.

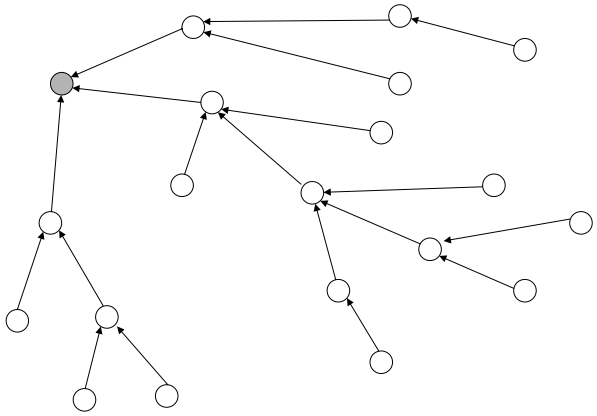


Figure 2.3: Routing tree

In the *geographic* or *greedy* routing all nodes are aware of its own location according to a coordinate system as well as their neighbours (each node periodically broadcasts its location to neighbours). On the basis of the destination location (carried in each packet) a node forwards packets to the neighbour that minimizes remaining distance [3]. Figure 2.4 illustrates greedy routing for the Euclidean distance routing. In the example node *x* chooses node *y* as the next hop for a message with destination *d*.

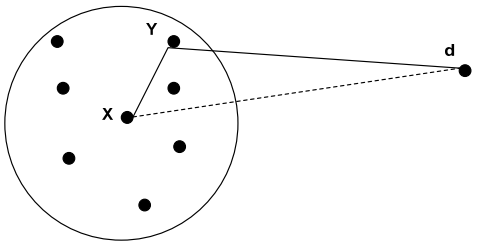


Figure 2.4: Greedy routing

The main deficiency of greedy routing is that it cannot guarantee delivery in every network topology and fails in the presence of voids or obstacles that introduce discontinuities in the topological connectivity structure. In fact it may lead packets into a dead end where a node cannot forward the packet since it is closer to the destination that any of its neighbours as illustrated in Figure 2.5. However, it is efficient in areas with nodes densely and regularly populated.

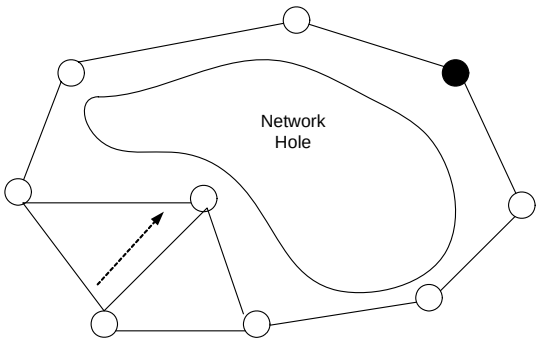


Figure 2.5: Dead end in greedy routing

Ideal routing protocols for WSNs should base routing decisions on information exchanged with neighbours, offer network reliability and require minimal message overhead, power consumption

and memory footprint. For these reasons most of the research on routing in WSNs has focused on localized or location-based protocols [3].

On top of that, in [6] has been shown that routing protocols that do not use geographical location information are not scalable.

In the rest of this section some *location-* or *geographic-based* routing protocols for WSNs are reviewed.

GPSR

The greedy perimeter stateless routing (GPSR) [34] protocol is a non-energy aware protocol that uses nodes location and packet destination to make packet forwarding decisions.

Under GPSR, packets are marked by their originator with their destination's locations. As a result, a forwarding node can make a locally optimal greedy choice in choosing a packet's next hop. Specifically, if a node knows its neighbours' positions, the locally optimal choice of next hop is the neighbour geographically closest to the packets' destination. Forwarding in this scheme follows successively closer geographic hops until destination is reached. However, a problem may occur when such a neighbour doesn't exist and the current node is closer to the destination than any of its neighbours (dead end). When a packet reach a dead end, the protocol switches to perimeter forwarding and uses the right hand rule to take tours of enclosed cycles in a planarized network graph.

Upon receiving a greedy-mode packet for forwarding, a node searches its neighbour table for the neighbour geographically closer to the destination. If this neighbour exists the node forwards the packet to it, otherwise, the node marks the packet into perimeter mode. GPSR forwards perimeter-mode packets using a simple planar graph traversal (a graph in which no two edges cross). Perimeter forwarding is only intended to recover from a local maximum; once the packet reaches a location closer than where the greedy forwarding previously failed, the packet can continue greedy progress toward the destination without danger of returning to the prior local maximum.

GPSR and other similar algorithms based on graph planarization are not perfect. Inaccuracies in position estimates and irregular radio ranges (possible due to obstacles) may result in errors in the planarization procedure causing routing failures and infinite loops [3]. On top of that, this recovery procedure requires calculating and maintaining planar graphs information at every node, which is highly inefficient given that this information is rarely used [35].

GAF

The *Geographic Adaptive Fidelity* (GAF) [36] protocol is an energy-aware location-based routing algorithm originally designed for ad hoc networks but applicable to sensor networks as well.

The protocol first divides the network into fixed zones and forms a virtual grid. Inside each zone, nodes collaborate with each other to play different roles conserving energy by turning off unnecessary nodes without affecting the level of routing fidelity. Each node uses its GPS-indicated location to associate itself with a point in the virtual grid. Nodes associated with the same point on the grid are considered equivalent in terms of the cost of packet routing. Such equivalence is exploited in keeping some nodes located in a particular grid area in sleeping state in order to save energy. Thus, GAF can substantially increase the network lifetime as the number of nodes increases. Nodes change states from sleeping to active in turn so that the load is balanced.

A sample situation is depicted in Figure 2.6. Here, node 1 can reach any of 2, 3 and 4 and 4 can reach 5. Thus, nodes 2, 3 and 4 are equivalent and two of them can sleep.

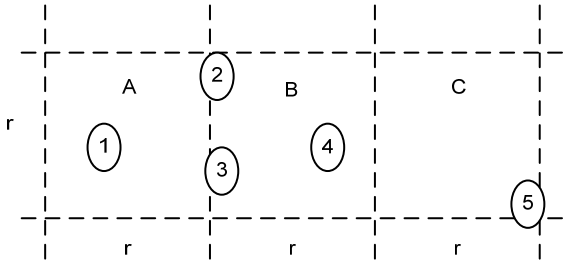


Figure 2.6: Example of virtual grid in GAF [36]

As illustrated in Figure 2.7, GAF defines three states: *discovery*, for determining the neighbours in the grid; *active*, reflecting participation in routing; and *sleep*, when the radio is turned off. Which node will sleep for how long is application dependent and the related parameters are adjusted accordingly during the routing process.

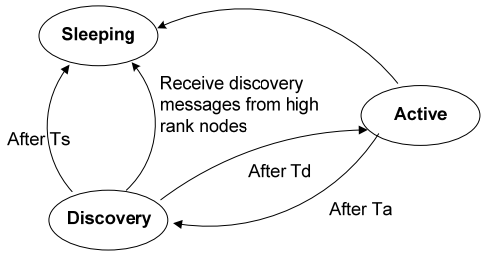


Figure 2.7: State transitions in GAF [4]

GAF strives to keep the network connected, by keeping a representative node always in active mode for each region on its virtual grid.

Simulation results show that GAF performs at least as well as other ad hoc routing protocols in terms of latency and packet loss, and increases the lifetime of the network by saving energy.

Although GAF is a location-based algorithm, it may also be considered as a hierarchical protocol.

2.6 Sensor networks based on smart antennas

2.6.1 Definition and overview

Smart antenna is one of the most promising technologies that enables a higher capacity in wireless networks by effectively reducing multi-path and co-channel interference [37, 38]. Multipath is a condition where the transmitted radio signal is reflected by physical features/structures, creating multiple signal paths between the base station and the user terminal. For its part, co-channel interference occurs when the same carrier frequency reaches the same receiver from two separate transmitters [39].

This reduction is achieved by focusing the radiation only in the desired direction and adjusting itself to changing traffic conditions or signal environments. A smart antenna system combines multiple antenna elements with a signal processing capability to optimize its radiation and/or reception pattern automatically in response to the signal environment. Smart antennas systems are categorized as either *switched beam* or *adaptive array* systems.

Switched beam antenna systems form multiple fixed beams with heightened sensitivity in particular directions. These antenna systems detect signal strength, choose from one of several predetermined fixed beams, and switch from one beam to another as the mobile moves throughout the sector. In an adaptive array antenna system, by the means of an adaptive

algorithm, the adaptive systems takes advantage of its ability to effectively locate and track various types of signals to dynamically minimize interference and maximize intended signal reception [7, 39].

Although both systems attempt to increase gain in the direction of the user, only the adaptive array system offers optimal gain, while simultaneously identifying, tracking, and minimizing interfering signals [39, 40]. It is the adaptive system's active interference capability that offers substantial performance advantages and flexibility over the more-passive switched-beam approach [41].

2.6.2 Smart antenna systems in sensor networks

Until recently, research in smart antenna systems in the area of sensor network has been prohibitive due to size, cost, and power considerations. Smart antenna technology implemented within sensor network hardware platforms seems contradictory. On the one hand, sensor nodes are extremely sensitive to power consumption, computational power, size and cost. On the other hand, smart antenna systems not only require larger amount of space (to handle multiple antenna elements), but also more computational power (since signals from the set of antenna elements are processed and controlled in order to make communication more efficient), and more electronics capable of translating radio frequency (RF) signals to baseband signals suitable for processing [10].

Conversely, the use of smart antennas in sensor nodes is not only feasible, but also desirable. As sensor node dimension shrinks, RF communication will be forced to utilize higher frequencies. Fundamental theory states, however, that transmission using higher frequencies results in lower effective communication ranges. To compensate for distance loss, higher gains have to be achieved. Increased gains, which can be attained using smart antennas, are necessary to preserve connectivity in networks and efficiently use a sensor node's energy source [9, 10]. The advantages of using smart antennas in ad-hoc communications has been demonstrated using small-scale and large-scale fading models in [42] where improvements of 20dB in received signal noise ratio (SNR) can be realized and the bit error rate can be reduced by more than 60%. Moreover, the use of smart antennas can be significantly decrease the nodes' power consumption, and therefore increase their lifecycle [9]. In addition, according to [10], integrating the smart antenna scheme into the sensor hardware platform increases the total cost of the design by only 3%.

In [9], the authors propose a new family of protocols that try maximizing efficiency and minimizing energy consumption by favouring certain paths of local data transmission towards the sink by using switched beam antennas at the nodes. Just like flooding, the protocol requires nodes to forward every new incoming packet, avoiding network resources depletion by restricting the nodes that receive and hence retransmit the message with the use of switched beam antennas.
The mechanism that controls this propagation of information is the following; during the initialization phase of the network, the base station transmits a beacon frame with adequate power to be able to reach all the network's nodes. Each node switches among its diverse beams and finds the one that delivers the best signal. After the initialization phase, the nodes will use this beam only for transmitting data, and they will use the beam lying on the opposite side of the plane only for receiving data. During normal operation, nodes retransmit every new incoming packet that has not received before. Figure 2.8 shows a conceptual representation of the protocol.

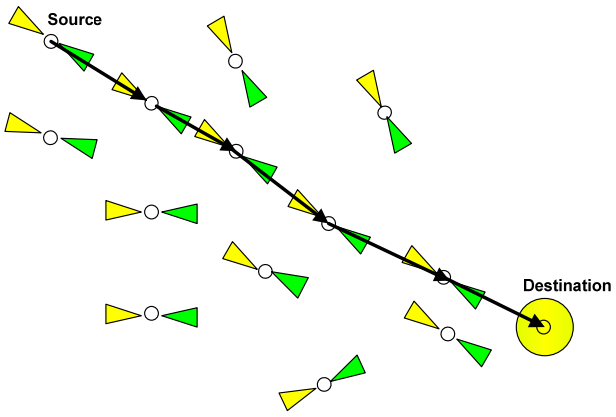


Figure 2.8: Delivery of information using smart antennas

2.7 The ZigBee Standard

As mentioned in section 2.4, ZigBee [30] is the name of a specification for a suite of high level communication protocols for reliable, cost-effective and low power wireless networking that has great possibilities in wireless monitoring and control applications. ZigBee technology will probably be embedded in a wide range of products and applications across consumer, commercial, industrial and government markets worldwide[3].
ZigBee defines the network, security, and application profile framework layers for an IEEE 802.15.4-based system [31] which defines the physical (PHY) and medium access control (MAC) layer for Wireless Personal Area Networks (WPANs).

The application layer defines the corresponding application specification for different background. The application profile framework allows different developers to independently build and sell ZigBee devices that can interoperate with each other in a given application profile. For its part, security services provided for ZigBee comprise methods for key establishment, key transport, frame protection, and device management.

The definition of the ZigBee network layer includes network topology, network establishment, the discovery and maintenance of routes between devices, the discovery of one-hop neighbors and the storing of relevant neighbor information.

ZigBee identifies three network topologies: star, tree and mesh topology, and defines three network devices: a ZigBee End Device (ZED), a ZigBee Router (ZR) and a ZigBee Coordinator (ZC).

ZEDs are equipped with sensors and contain just enough functionality to talk to the parent node (either router or coordinator) being enable to relay data for other devices. This fact allows the node to be asleep a significant amount of time thereby giving long battery life. It is also the device that requires the least amount of memory.

ZRs besides of having sensors are also equipped with a full set of MAC layer functions which allows them to act as intermediate routers passing data from other devices as well as running application functions.

The ZC is a single device on each network responsible for initiating and maintaining devices on the network, choosing certain key network parameters and acting as the trust centre and repository for security keys. The ZigBee Coordinator forms the root of the network tree and might bridge to other networks.

The star topology of ZigBee is mainly designed for the simple communication from one node to several nodes, the tree network uses a Hierarchical/Tree Routing mechanism and the mesh network uses the mixed routing method combined with AODV and Hierarchical/Tree routing.

2.7.1 Network Formation and network assignment

When a device *c* wants to join an existing network, the network layer is requested to start a network discovery procedure which allows *c* to discover neighboring routers announcing their networks. After the upper layers have decided which network to join (several ZigBee networks may overlap spatially, using different channels), the network layer selects a “parent” node *p* (in the desired network) from his neighborhood, and asks the MAC layer to start an association

procedure. Upon receiving an indication of the association request from the MAC layer, *p*'s network layer assigns *c* a 16-bit short address and lets the MAC layer successfully reply to the association request. Node *c* will use the short address for any further network communication.

Parent-child relationships shape the whole network in the form of a tree with the ZC as the root, the ZRs as internal nodes and ZEDs as leaves. This tree structure is also at the basis of the distributed algorithm for network address assignment. The ZigBee fixes the maximum number of routers (R_m) and end-devices (D_m) that each router may have as children and also fixes the maximum depth of the tree (L_m). On the basis of this depth in the tree, a newly joined router is assigned a range of consecutive addresses (16-bit integers). The first integer in the range becomes the node address while the rest will be available for assignment to its children (routers and end-devices). The size *A(d)* of the range of addresses assigned to a router node at depth $d < L_m$ is defined by the following recurrence:

$$A(d) = \begin{cases} 1 + D_m + R_m & \text{if } d = L_m - 1 \\ 1 + D_m + R_m A\,(d+1) & \text{if } 0 \le d < L_m - 1 \end{cases}$$

Nodes at depth L_m and end-devices are obviously assigned a single address. The recurrence is easily solved and used by each router to assign addresses to its children. Assume that a router at depth *d* receives the range of addresses $[x,\ x + A(d)]$. It will have address *x* and it will assign range $[x + (i\text{-}1)\ A(d+1) + 1,\ x + i + A(d+1)]$ to its *i*-th router child ($1 \le i \le R_m$) and address $x + R_m\ A(d+1) + j$ to its *j*-th end-device child ($1 \le j \le Dm$).

Figure 2.9 extracted from [3] illustrates an example network with $R_m = 2$, $D_m = 2$ and $L_m = 3$ where all addresses have been assigned to routers (white nodes) and end-devices (gray nodes). The address appears inside the circle representing each node, while the assigned address ranges are displayed in brackets next to each router. ZigBee's addressing scheme can support up to 65.535 nodes per coordinator, and multiple coordinators can be linked together to increase the overall network size.

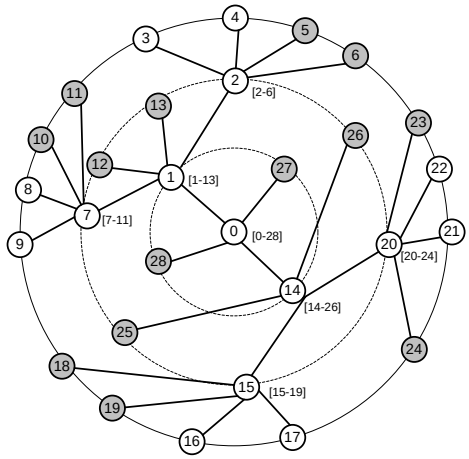


Figure 2.9: Address allocation for Rm = 2, Dm = 2 and Lm = 3

Defining different network devices, each one with particular technical specifications and a precise role within the network is a serious inconvenience when the sensor's deployment is random, since in this situation it is not possible to control where the devices will be located.

2.7.2 Routing

As previously mentioned, the routing algorithm depends on the topology used in the sensor network. In a *tree topology*, routing is limited to parent-child links established as a result of join operations. Routers maintain their address and the address information associated with their children and parent. Given the addressing system, a router that needs to forward a message can easily determine if the destination is one of its children. If so, it routes the packet to the appropriate child; otherwise it routes the packet to its parent.

In the *mesh network*, routers maintain a routing table (RT) and employ a route discovery algorithm to construct/update these data structures on the path nodes. A routing table entry (simplified version) is described in Table 2.1.

Table 2.1: ZigBee routing table

Field Name	***Description***
Destination Address	*16-bit network address of the destination*
Next-hop Address	*16-bit network address of next hop towards destination*
Entry status	*Status of the route: Active, Discovery or Inactive*

Figure 2.10 illustrates a simplified version of the algorithm used to route a packet.

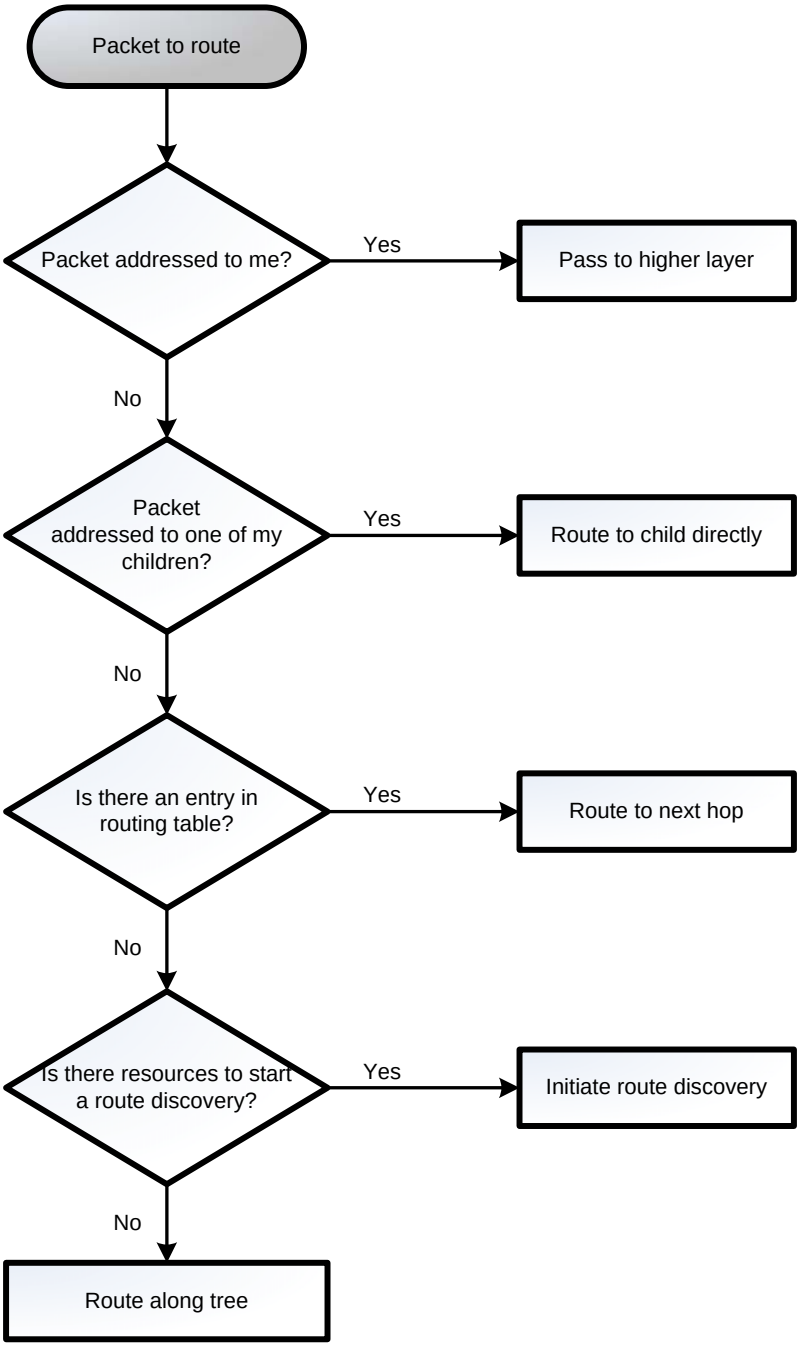


Figure 2.10: Routing protocol

When trivial routing is not possible, the routing table is consulted for the next hop to destination. If there is no entry, the network layer attempts to start the route discovery procedure. In case sufficient resources are not available for the process it falls back to tree base routing.

2.7.2.1 Route discovery

Route discovery is a process that allows establishing RT entries in the nodes along the path between two nodes wishing to communicate. In ZigBee, route discovery is based on the Ad hoc On Demand Distance Vector routing algorithm (AODV) [28].

In order to store temporary information used during the route discovery process, the ZC and the ZRs in addition to the RT, also keep a Route Discovery Table (RDT) containing the information shown in Table 2.2.

Table 2.2: Content of the Route Discovery Table

Field Name	***Description***
RREQID	*Sequence number for a RREQ command frame. Incremented each time a device initiates a RREQ*
Source Address	*network address of the RREQ initiator*
Sender Address	*Network address of the device that sent the most recent lowest cost route request*
Forward Cost	*The accumulated path cost from the RREQ initiator to the current device*
Residual Cost	*The accumulated path cost from the current device to the destination device*
Expiration Time	*A countdown timer indicating number of milliseconds until route discovery expires*

When a node needs to communicate with a certain destination, it broadcasts a route request (RREQ) message that propagates through the network until it reaches the destination. Every RREQ contains an ID (incremented by the originator every time it sends new RREQ messages), used in conjunction with the source address to uniquely identify each routing discovery process. While circulating, the RREQ accumulates a *forward cost* value that corresponds to the sum of the cost of all the links it traversed (the cost of a link can be set to a constant value or be dynamically calculated based on a link quality estimation provided by the IEEE 802.15.4 interface).

The reception of an RREQ triggers a search within the RDT for an entry matching the route discovery. If the entry is found, the node compares the RREQ's *forward cost* to the corresponding value in the RDT entry. If it is higher it drops the RREQ message, otherwise it updates the RDT entry. In case no match is found, a new RDT entry is created for the discovery process. Finally, if the current node is not the destination, it assigns an RT entry for the destination with status *Discovery* and rebroadcasts the RREQ after updating its *forward cost*

field. If the node is the final destination, it replies to the originator with a route reply (RREP) massage that travels back along the path. Figure 2.11 illustrates the RREQ process.

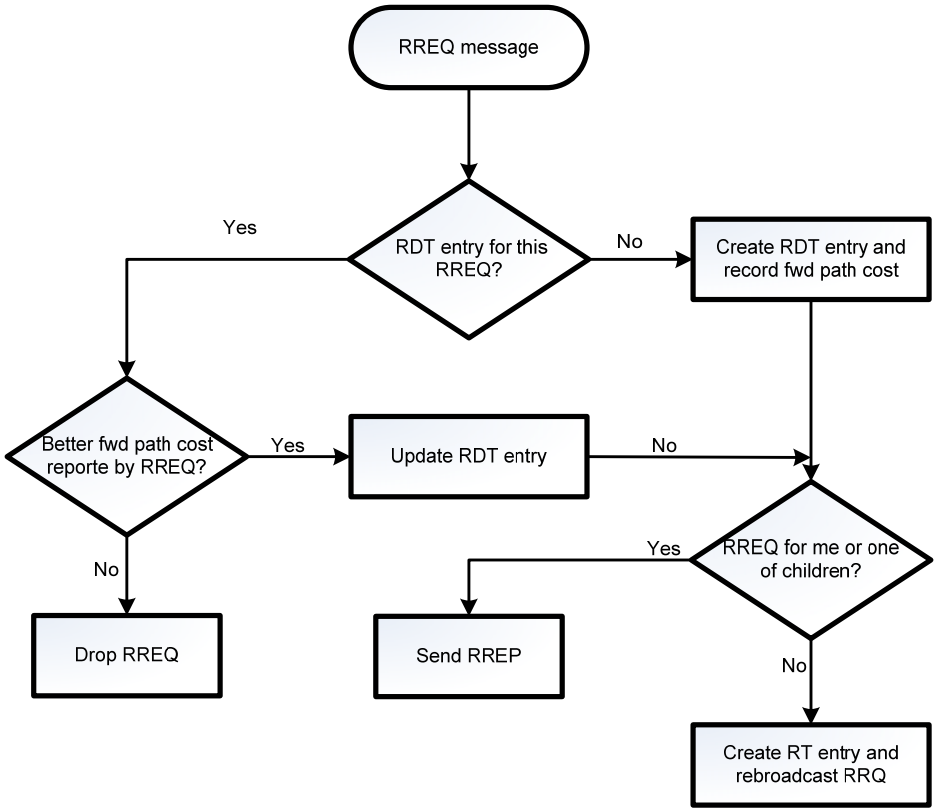


Figure 2.11: RREQ processing

The RREP message is addressed to the route discovery originator and carries with a residual cost value field that each node increments as it forwards the message. Upon receipt of a route reply (RREP) message, a node retrieves the RDT and RT entries for the associated route discovery. If the node is the RREQ originator and this is the first RREP it receives, it sets the RT entry to Active and records the residual cost and next hop in the RDT entry. In all other cases it compares the residual cost from the RREP with the one from the RDT entry. If the former is higher the node discards the RREP message; otherwise it updates the RDT entry (residual cost) and the RT entry (next hop). A node that is not the RREP originator must also forward the RREP towards the originator. Intermediate notes never change the entry status to Active as a result of receiving a RREP message. They will only change the status upon reception of a data message for the given destination. Figure 2.12 illustrates the RREP message processing.

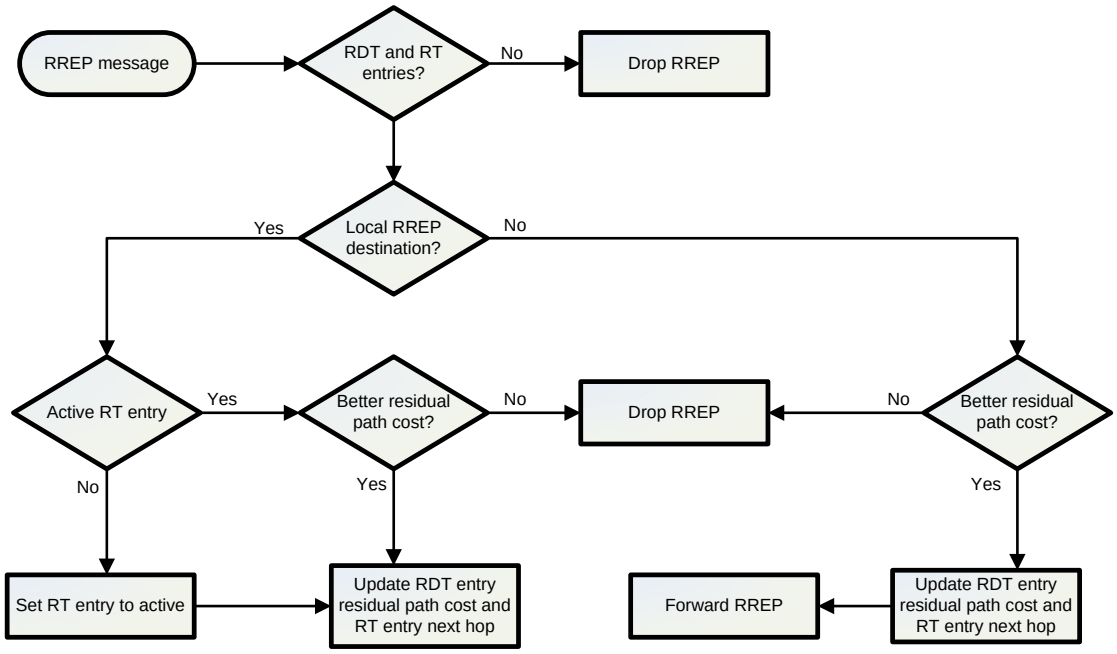


Figure 2.12: RREP processing

CHAPTER 3 PROPOSED LOCATION ROUTING ALGORITHM BASED ON SMART ANTENNAS FOR WIRELESS SENSOR NETWORKS

The previous chapter introduced main of the existing routing strategies for wireless sensor networks and exposed the reasons for which data routing in this type of networks supposes a true challenge. In the same way, recent advances reached in the implementation of smart antenna technology within sensor networks were presented.

The use of smart antennas enables a higher capacity in wireless networks by effectively reducing *multipath* and *co-channel interference*, improving network communication and decreasing power consumption, thus increasing its lifecycle. Additionally, they allow making an accurate estimation of nodes positions without requiring additional components.

In this chapter, we analyze main performance criteria required to evaluate routing protocols for wireless sensor networks and present the Location Based Routing Algorithm (LBRA) as an enhanced version of the ZigBee routing. The changes proposed concern the synchronization of the location information, broadcasting mechanisms, and balancing the power consumption in order to make the protocol energy aware.

3.1 WSNs routing protocols performance criteria

WSN is the latest family of wireless networks that has some distinctive characteristics (see section 2.4) which introduce additional requirements on its routing protocols. While conventional routing protocols for wireless networks are typically only concerned with data throughput and network latency [43-46] , efficient and reliable routing protocols in WSNs have to satisfy the following performance criteria [1, 4, 47]:

- ***Efficiency in energy consumption***: nodes are battery operated and network lifetime depends on battery lifetime. The routing protocol must be energy-efficient by minimizing energy consumption to maximize network lifetime.
- ***Tolerate node failures***: nodes are prone to failures that could render them useless either on a temporary or permanent basis leading to frequent topology changes. The routing protocol must react to the change in topology quickly and reduce the impact on general network performance by discarding the invalid route and obtaining a new one.

- ***Guaranteed delivery***: cheap and low-powered transceivers used by WSN nodes exacerbate the inherently unreliable RF medium. Consequences are high packet loss and error rates and intermittent disruptions to communications. The routing protocol must operate under such conditions to achieve efficient and reliable message delivery.
- ***Scalability***: the number of sensor nodes in a sensor field might reach the order of millions. Routing protocols must therefore be scalable by having low routing overheads and maintaining consistent performance when the network size increases.
- ***Loop-free transmission***: loops can happen when a package remains spinning arbitrarily in a circle formed by certain nodes. Routing protocols must be able to avoid these errors to occur.
- ***Security***: given that WSNs are limited in computational power and communication resources, existing network security mechanisms are inappropriate for this kind of networks. Efficient encryption of measured data can be achieved at the cost of increased overheads in the length of the message. But as radio communications is the most energy consuming function performed by these nodes, hence the communications overheads have to be minimized to achieve long life [48].

The security requirements of wireless sensor networks are [49]:

- ***Data confidentiality***: means keeping important transmitted information secret from unauthorized people. It is usually achieved by encrypting the information before transmission.
- ***Data authenticity***: provides a means to detect messages from unauthorized nodes thereby preventing unauthorized nodes to participate in the network.
- ***Data integrity***: provides a way for the receiver of the message to know if the data has been tampered while in transit by an attacker.
- ***Data freshness***: ensures that the received data is recent and that the adversary has not replayed old messages at a later time.

Additionally, and given that sensor networks are application specific, there are other criteria to evaluate a protocol performance such as:

- ***Quality of Service***: in some applications data should be delivered within a certain period of time from the moment its sensed or it will be useless. Therefore, bounded latency for data delivery is another condition that routing protocols must guarantee.

- ***Node heterogeneity***: depending on the application a sensor node can have a different role or capability that raises many technical issues related to data routing. For example, some applications might require a diverse mixture of sensors for monitoring temperature, pressure, and humidity of the surrounding environment, detecting motion via acoustic signatures, and capturing images or video tracking of moving objects. In this case, data reading and reporting can be generated at different rates, subject to diverse QoS constraints, and can follow multiple data delivery models.

Although ideally a routing algorithm for WSNs should satisfy all the performance criteria mentioned above, in the practice is almost impossible especially if we consider that sensor networks are application specific and routing decisions will be made based on the particular application requirements. The novel algorithm will satisfy following criteria: *loop free transmission, efficiency in energy management, scalability, node failure tolerance, node heterogeneity and guaranteed delivery*.

Regarding security, WSNs are especially vulnerable to a variety of attacks due to the broadcast nature of the transmissions and because nodes are often placed in a hostile or dangerous environment without physical protection. Also, the close interaction of sensor nodes with their physical environment and with people, poses new security problems that require very special attention. These factors combined with the restrictions imposed by the intricate nature of sensor networks, make the security issue a vast subject in its own right, complex enough to merit separate research and consequently is left for future investigation.

As for QoS, it is not considered in this work for two reasons: (1) given that QoS is application dependant, it is not feasible to define an all-purpose protocol that fulfills all possible constraints and in this work we are not considering a specific type of application but a general case. (2) Mechanisms used by LBRA introduce delays that make difficult guaranteeing the QoS, especially regarding the end-to-end delay.

3.2 Location aided Routing in WSNs

Geographic routing requires only accurate neighbourhood information and a rough idea of the position of the destination eliminating the necessity to set up and maintain explicit routes, reducing communication overhead and routing table size. Hence, allowing routers to be nearly stateless and requiring propagation of topology information for only a single hop. These

advantages allow scalability especially in dynamic, critically power constrained and unstable wireless networks[5, 50].

As studied in section 2.4.3, it has been experimentally confirmed that routing protocols that do not use geographic location in the routing decisions are not scalable [6] and therefore, most of the research on routing in WSNs has focused on localized protocols resulting in the proposal of several location-based routing algorithms.

Absolute position Vs. Relative position

One possibility to deal with the location problem would be to manually assign node's location, which is often impractical or impossible due to the number of nodes or the method of deployment.

Another option could be to equip all nodes with a GPS receiver which will provide the *absolute or global position* of each node. However, this is an expensive solution due to GPS receiver's costs, power consumption and size requirements which are inappropriate for resource-constrained networks. It may also fail to work if some nodes cannot receive GPS signals (for example it cannot be used for indoor applications).

A cheaper alternative would be to equip with GPS receivers (or manually provide correct coordinates) only a few anchor nodes and, according to these, approximate the coordinates of other nodes.

Absolute (or global) position approach is very effective at locating data sources but requires expensive and complex hardware and protocols. Additionally, it might suffer from important measurement and approximation errors and may lead to stuck nodes when combined with greedy routing since geographic proximity doesn't necessarily means topological proximity [3]. As an alternative, it is possible to use *relative or local positioning.*

In relative localization, neighbouring nodes can measure the distance between them through communication, and based on these distances all nodes can estimate their relative positions in relation to each other using distributed localisation algorithms [51]. Some applications need absolute positions in order to work properly; however, many applications require only the knowledge of the node's relative position.

There are different techniques for position location that take advantage of the actual micro-sensor technology. Among them we find [51, 52]: t*ime of arrival* (ToA) which measures the radio signals' propagation time, *time difference of arrival* (TDoA), a special case of ToA, which

estimates the distance from propagation times through different media (such as radio and ultrasound), *angle of arrival* (AoA), proposed to estimate relative angles between neighbours and *received signal strength indicator* (RSSI), highly supported by current transceivers since it doesn't require extra equipment and consequently commonly adopted by many localisation systems.

Based on reliance on the hardware support, localisation algorithms can be classified into two main categories: *range-based* algorithms and *range-free* algorithms. Range-based algorithms rely more on hardware support by applying either one or a combination of ToA, TDoA, AoA or RSSI technologies. On the contrary, range free algorithms require less or no hardware support at all [51].

Smart antennas receive radio signals and collect information such as *AoA*, *TDoA* and *phase of the signal at arrival* and process it by the means of an embedded digital circuit being only able to locate nodes in their range. Thus, when combined with a relative-position based routing algorithm, a node knows its neighbours' status of connections and relative positions, which makes the route decision making process very simple. By contrast, in a global-position based routing algorithm, before route decisions can be made, nodes must synchronize the global position throughout the network, calculate the network coordinates and work out the connectivity map (highly variable), which makes the routing decision process more complex [53].

Due to the limits imposed by the use of absolute position in highly constricted networks such as WSNs and considering the technical specifications of smart antennas previously described, in this work we propose to use relative position.

Location Estimation

So far, many location estimation methods, based on the location techniques enunciated in the previous section, have been proposed. Among them we find, maximum likelihood estimation, Capon's minimum variance method (MVDR)[54, 55] and subspace based estimation (MUSIC and ESPRIT)[54-57]. In this work, we measure signal parameters through the MUSIC algorithm. The MUSIC algorithm is a subspace based high resolution multiple signal classification technique that can be used to accurately estimate the number of incident signals and the direction of arrivals of the signals by exploiting the Eigen-structure of the input covariance matrix. The term "high-resolution" refers to the fact that the frequency estimation or angle of arrival estimation has, under carefully controlled conditions, the ability to surpass the limiting behaviour

of classical Fourier-based methods [58]. This algorithm divides the space spanned by the Eigen vectors of the input covariance matrix of the received signal into two subspaces - signal plus noise subspace and the noise subspace.

Assumptions

A few assumptions before presenting our solution:

1 All nodes are equipped with smart antennas, thus being able to identify their neighbor's connection status and relative position by the incoming radio waves.
2 All nodes in the network are energy constrained.
3 All nodes in the network play the same role within the routing process, which essentially means that every sensor node is able to perform routing tasks.
4 Each sensor node is outfitted with a battery and in the beginning all nodes in the sensor field have the same energy level.
5 All nodes have a mechanism to know the remaining battery level.

3.3 The location based routing algorithm (LBRA)

The main purpose of the LBRA is to eliminate network control overhead as much as possible. To achieve this goal, the algorithm employs local position for route decision, implements a novel mechanism to collect the location information and involves only route participants in the synchronization of location information. In addition, the protocol uses node battery information to make power aware routing decisions.

LBRA is prototyped from AODV (which has become a milestone of reactive algorithms) and has three parts: Route Discovery (RD), in which nodes seek routes to communicate among themselves, Route Establishment (RE), in which nodes set up two-way connections by the exchange of the required information, and Route Maintenance (RM), that poses a mechanism to select the best route in terms of energy consumption among the routes found during the Route Discovery stage. The Route Discovery in its turn is divided into two stages: Route Request (RREQ), in which a source node searches for a specific destination node in the network, and Route Reply (RREP) that allows, once the destination node is found, the establishment of the two-way communication path between the nodes.

Every node will have a Routing Table (RT) and a Route Discovery Table (RDT) that will be constructed/updated during the RD phase. The basic information contained in the RT and in the RDT is shown in Table 3.1 and Table 3.2 respectively.

Table 3.1: LBRA routing table

Field Name	***Description***
Destination Location	*Location of the destination node*
Pre-hop Address	*Location of the previous hop from the source*
Next-hop Address	*Location of the next hop towards destination*
Entry status	*Status of the route: Active, Discovery or Inactive*
Expiration Time	*A countdown timer indicating the number of milliseconds until the route entry expires*

Table 3.2: LBRA route discovery table

Field Name	***Description***
RREQID	*Sequence number of the RREQ message*
Source Address	*Location of the RREQ initiator*
Sender Address	*Location of the device that sent the most recent lowest cost route request*
Relay Cost	*The accumulated path relay cost from the RREQ initiator to the current device*
Reverse Relay Cost	*The accumulated path cost from the current device to the destination device*
Expiration Time	*A countdown timer indicating number of milliseconds until route discovery expires*

3.3.1 Route Discovery

Route Discovery (RD) is a process that allows nodes to collect and record the necessary information to communicate or to act as relay entities according to the case. In this stage, RT and RDT entries in the nodes along the path between two nodes wishing to communicate are created. In LBRA there are two possible scenarios for the RD process: flooding and limited flooding (concept originally proposed in [59] for mobile ad hoc networks). The choice of the scenario will depend on the awareness of the destination node's position: if the source node knows the location of the destination node, it uses the limited flooding; otherwise, it floods the entire network.

The propagation algorithm to flood the network is similar to the one used by the ZigBee RD. When a source node S needs to communicate with a certain destination node D, it broadcasts an RREQ message to all its neighbors. Each *route request* message is uniquely identified by a conjunction of the *Source Node Identifier* (SID), *Destination Node Identifier* (DID) and an RREQ *Identifier* (RREQID) that is incremented by the originator every time it sends a new RREQ message. Upon reception of the RREQ, a node J compares the DID with its own ID. If they match, it means the request was looking for a route to itself; otherwise J forwards the RREQ to its neighbors. To avoid loops, before forwarding the packet, J (acting as an intermediate node) verifies the SID, DID and RREQID to check if the message has been previously received. If so, the redundant RREQ is dropped. Figure 3.1 illustrates the flooding algorithm.

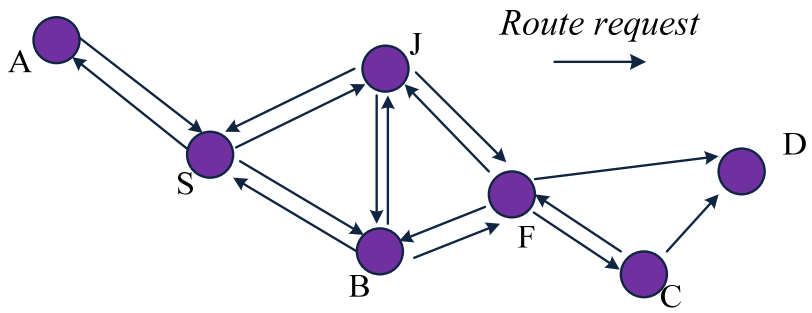


Figure 3.1: Flooding

In the example, S needs a route to communicate with D and thus it broadcasts an RREQ to all nodes in its vicinity. Upon reception of the request, nodes J and B forward it to all their neighbors. In turn, when node F receives the RREQ from B it sends the message to its neighbors. However, when the request comes from J, F detects that is a duplicate and discards it.

Given that the *route request* is disseminated to several nodes by using the flooding algorithm, the path followed by the message must be included in the RREQ packet. Once the route request is received by the destination node, it responds to the originator by sending a *route reply* message using the reverse path followed by the *route request* received.

It is always possible that the destination node doesn't receive a *route request* message due to different circumstances such as transmission errors or because the destination node might be unreachable from the sender at a certain moment. In order to control that, when launching a *route discovery*, the sender sets a timeout. If by the end of this time out no reply message is

received, a new *route discovery* request is started. Time-out may also arise when the *route reply* message from the destination is lost.

The *route discovery* process is started either when the source node doesn't know a route to reach the destination node, or when a route previously established between them is not longer available. In this latter situation, since nodes have already had communication, location information is available and instead of flooding the whole network looking for a route, LBRA will switch to the limited flooding scenario, restricting the flooding to a specific area called the *Target Zone*.

Let's consider a node S that needs to set up a route to node D whose position already knows. In this case, node S defines a *Target Zone* for the *route request,* sending the message only to certain neighbor nodes located within a *"cone"* [60] that has S as its vertex, the line connecting S and D as its axis and the initial opening angle of 20°. Figure 3.2 illustrates the *Target Zone* setup for the limited flooding.

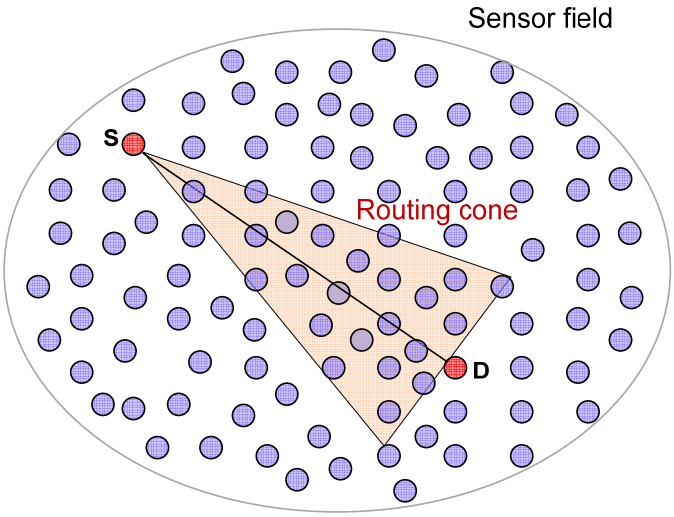


Figure 3.2: Target zone setup for the limited flooding

If after a suitable timeout period (calculated experimentally) a route between nodes S and D has not been discovered, the node S will start a new *route request* with an extended *target zone*. The way to extend the *target zone* is widening the opening angle of the "cone". In this case, however, the latency in determining the route from S to D will be higher since more than one *route request* will be necessary.

The source node will recognize that a route is broken if, by sending a data packet to the destination node, it receives a *route error message*. A node J belonging to that route will send a

route error message if upon reception of a data packet the next hop on the route is broken. As soon as the source node gets the *route error message*, it triggers a *route discovery* for destination D, using the limited flooding scenario.

To be able of determining whether the next hop on the route is working properly or not, every node will send periodic *hello* messages, with frequency **hello_time**, to the nodes that appear in its routing table as pre-hop (i.e. predecessors), only in *Active* routes; the neighbors that receive this packet keep record of the connectivity information. Failing to receive **max_hello_loss** consecutive hello message is an indication that the next hop is out of order and therefore, in the event a data packet must be transmitted to it, a route error message will be generated in return.

Having described the propagation method used to flood the network in either scenario available for the RD phase, in the following section we will discuss the *route request* message in detail.

3.3.1.1 Route Request

In LBRA, besides setting up connections between nodes, the flooding is also used to synchronize the location information throughout the network.

Initially, a source node S wanting to communicate with a destination node D will be unaware or poorly aware of the distribution of the network. Hence, when S triggers the *route request*, it will set its location as $P_S^S(0,0)$ in the RREQ and the position information will be updated hop by hop until the packet arrives at the destination node D [53]. Figure 3.3 illustrates an example of the synchronization procedure of a network with 4 nodes.

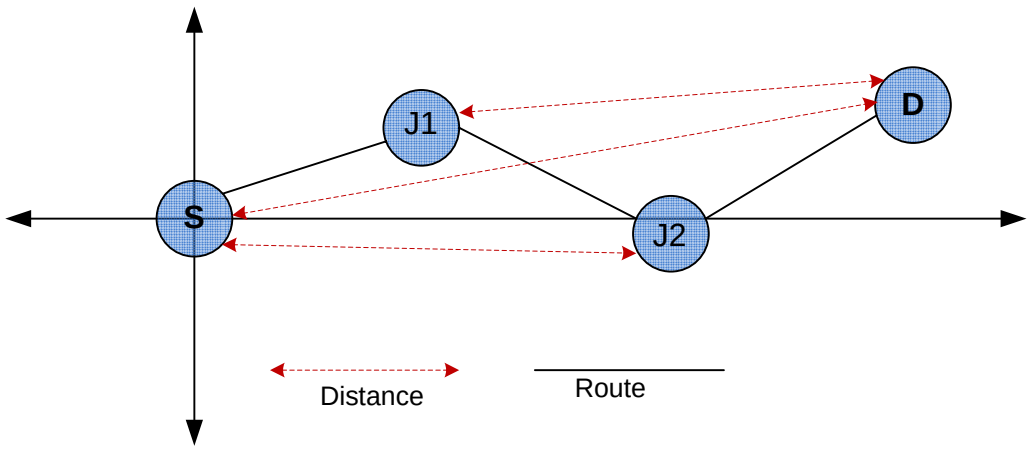


Figure 3.3: Location synchronization

To follow the example let's start with some definitions:

V: Represents the set of neighbors of a node

V_S: Represents the set of neighbors of node S

P_S^J: Represents the relative position of S in the coordinate system of node J

x_S^J: Position on the x axis of node S in the coordinate system of node J

$y_S^{J:}$ Position on the y axis of node S in the coordinate system of node J

$$P_S^J = (x_S^J, y_S^J)$$

Procedure:

1. S triggers a route request
2. Node J1 $\in$ Vs receives the RREQ and fixes the position of S with respect to its own coordinate system
3. Node J1 forwards the RREQ to its neighbor J2
4. Node J2 $\in V_{J1}$ receives the RREQ message and fixes the position of S by combining the position of J1, with respect to its own coordinate system, and the position of S with respect to the coordinate system of J1 included in the RREQ received. The calculation is made by formula 3.1.

$$P_S^{J2}(x_S^{J2}, y_S^{J2}) = P_{J1}^{J2}(x_{J1}^{J2}, y_{J1}^{J2}) + P_S^{J1}(x_S^{J1}, y_S^{J1}) \qquad (3.1)$$

$$\therefore P_S^{J2}(x_S^{J2}, y_S^{J2}) = P_S^{J2}(x_{J1}^{J2} + x_S^{J1}, y_{J1}^{J2} + y_S^{J1}) \qquad (3.1.1)$$

Following this procedure, location information is synchronized throughout the network and eventually, with the reception of the RREQ message, the destination node D will know the location of S with respect to itself and somehow the path that must follow to reach it. Location information will be used from that moment to make routing decisions.

An additional task accomplished by the RREQ message while circulating throughout the network, is to accumulate a *relay cost* value that corresponds to the sum of the cost of using the nodes belonging to the route that is being explored. If we define a route R of length L as a set of L nodes so that,

$$R = \{n_1, n_2, n_3, \ldots, n_L\}$$

And the link $\{[n_i, n_{i+1}]\}$ indicates that nodes n_i and n_{i+1} are direct neighbors (i.e. there is a link between them), the *relay cost* C{R} is defined by the equation

$$C\{R\} = \sum_{i=1}^{L} C\{[n_i, n_{i+1}]\} \quad (3.2)$$

Where $C\{[n_i, n_{i+1}]\}$ corresponds to the cost of traversing the link between n_i and n_{i+1}. The question now is how are we going to determine the cost of traversing a link?

As it has been widely discussed in previous sections, sensor nodes are extremely sensitive to power consumption, computational power, size and cost; being the efficient management of energy one of the most important issues when making decisions on network design and data routing. Consequently, to measure the energy consumption required by a node to relay information seems to be a natural choice to determine the cost of using a particular route.

Regarding energy consumption, the nodes on a sensor field can be in one of the following states: (1) transmission of a message, (2) reception of a message and (3) sensing of events. However, since our goal is to measure the cost of using a particular route, the only values that we are going to consider are those related to communication (transmission - reception).

To measure the energy dissipation for sensors we will use the first order radio model presented in [27]. According to this model, the energy spent by the transmitting node n_i to transmit a k-bit packet to its neighbor node n_{i+1}, separated from n_i a distance d, is

$$E_T(k,d) = E_{elec} * k + E_{amp} * k * d[n_i, n_{i+1}]^2 \quad (3.3)$$

And the energy spent by the receiving node n_{i+1} to receive a k-bit packet is

$$E_r(k) = E_{elec} * k \quad (3.4)$$

Where the constant $\boldsymbol{E_{elec}}$ corresponds to the energy dissipated to run the radio transmitter or receiver circuitry and the constant $\boldsymbol{E_{amp}}$ corresponds to the energy dissipated to run the transmit amplifier.

Deriving from the above equations, the cost incurred by the sensor node n_i for transmitting a k-bit packet is either:

$$C\{[n_i, n_{i+1}]\}(k) = 2 * E_{elec} * k + E_{amp} * k * d[n_i, n_{i+1}]^2 \quad (3.5)$$

or

$$C'\{[n_i, n_{i+1}]\}(k) = E_{elec} * k + E_{amp} * k * d[n_i, n_{i+1}]^2 \quad (3.6)$$

Where $C\{[n_i, n_{i+1}]\}$ is the cost of transmission between node n_i and node $n_{i+1}$for the relay packet, and $C'\{[n_i, n_{i+1}]\}$ is the cost of transmission for the generated data packet after sensing the environment, and $d[n_i, n_{i+1}]$ is the distance between nodes n_i and n_{i+1}.

RREQ process

Upon reception of an RREQ message, a node J searches within its RDT an entry matching the requirement. If the entry exists, J compares the relay cost stored on the table with the one of the RREQ received. If the former is lower the RREQ is discarded, otherwise the RDT entry is updated with data from the RREQ. In the case where no entry matches the RD, a new RDT entry is created.

At the end, J verifies whether the RREQ is addressed to itself (J is the destination node) or not (J is an intermediate node). If J is not the destination, it sets an RT entry for the destination node with status *Discovery* and broadcasts the RREQ to its neighbours (using flooding or limited flooding depending on the scenario). Otherwise, it replies to the RREQ sender with a *route reply* (RREP) message that travels along the reverse path followed by the RREQ. Figure 3.4 shows the REEQ process.

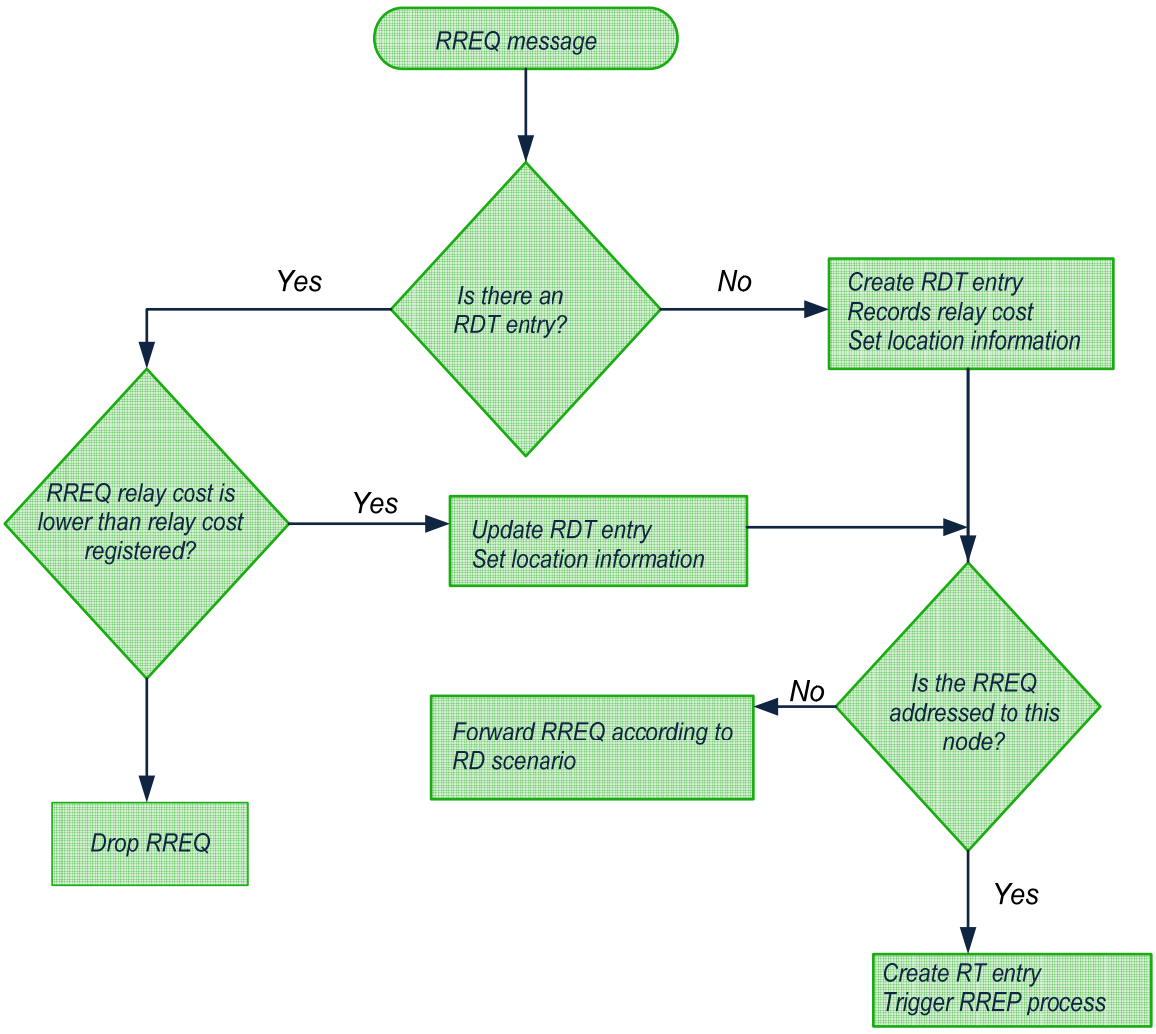


Figure 3.4: LBRA RREQ Process

3.3.1.2 Route Reply

The RREP message is created by the destination node and addressed to the originator of the RREQ to indicate that a route between them has been found. To reach the source node, the RREP simply backtracks the way followed by the RREQ message.

As the RREP message circulates on its way back to the source, all intermediate nodes will record the complementary data to establish the two-way path, so that the destination node can communicate with the source node.

In a similar way as with the RREQ, before sending the RREP towards the source, the destination node D sets its location information as $P_D{}^D(0,0)$ and the location of the source node, according

to what obtained in the calculations, as $P_S^D(x_s^D, y_s^D)$. Upon reception of the RREP, an intermediate node X transforms the location information to its own coordinate system, updates the RREP message and forwards it to the next hop. At a given time the RREP will reach the source node establishing a bidirectional route. Figure 3.5 show the RREP process.

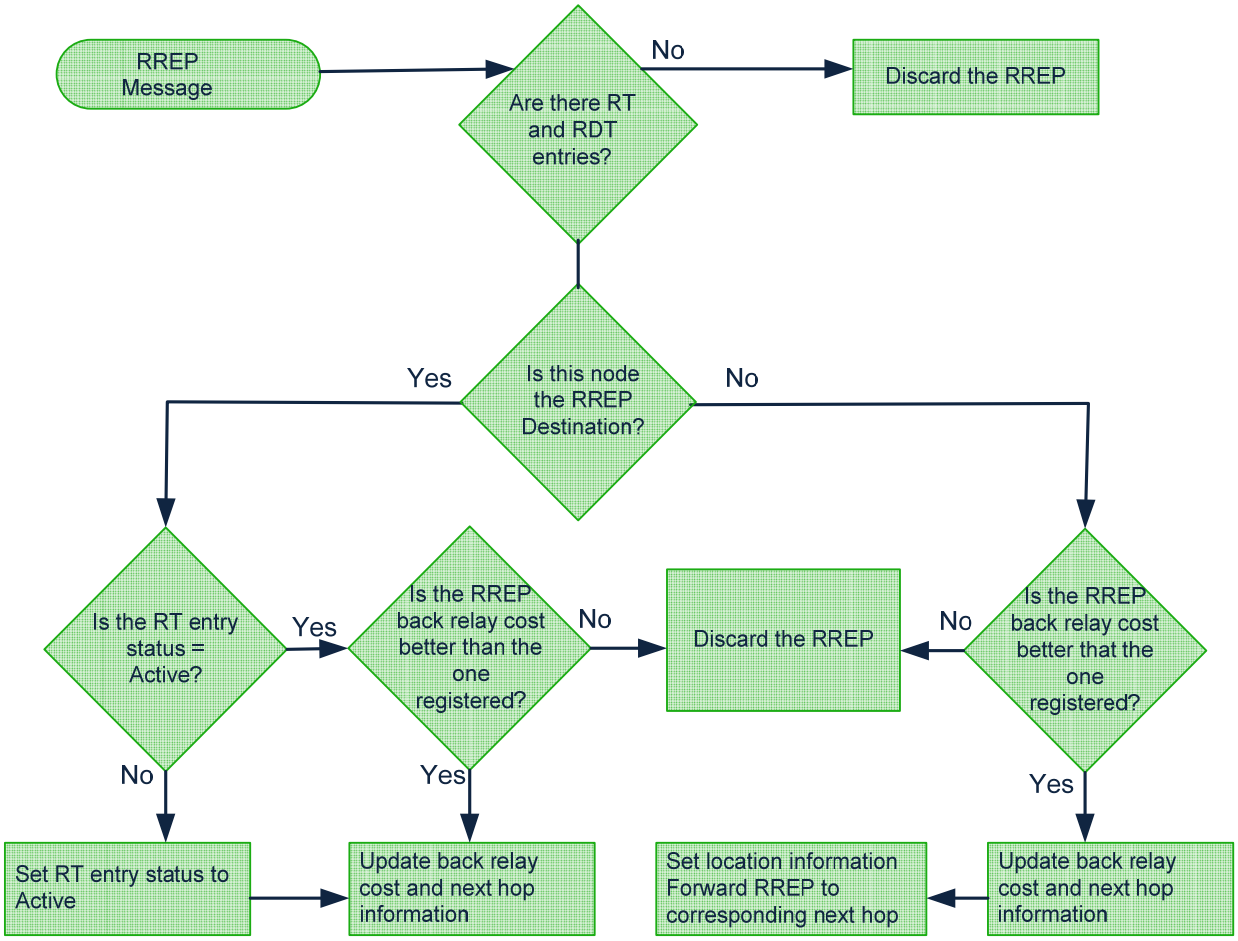


Figure 3.5: LBRA RREP process

3.3.2 Route Establishment

Upon reception of a route reply message (RREP), an intermediate node J retrieves the RDT and RT entries corresponding to the *Route Discovery* process that is being treated, and compares the *back relay cost* from the RREP with the one from the RDT entry. If the former is bigger, the RREP is discarded; otherwise the RDT (*back relay cost*) and the RT (*next hop, pre-hop*) entries are updated and the RREP is forwarded to the next hop.

When the first RREP message reaches the RREQ originator, this one sets the *Entry Status* of the RT entry to *Active* and updates the *back relay cost* and *next hop/pre-hop* information in the RDT and in the RT respectively. For all subsequent RREP messages, it compares the *back relay cost* with the one on the RDT entry, discarding the message or updating the tables as the case.
Intermediate nodes will only change the *Entry Status* to Active upon reception of the first data message for the given destination.

Routing table maintenance

In order to maintain the routing tables and minimize control overhead, each RT entry will have an *Expiration Time* field that will control the period of validity of the record. Every time a node sends (if it is the source node) or receives (in all other cases) a data packet, the expiration time of the corresponding RT entry is reset. In the event that the timer reaches zero and no data packet has being sent or received according to the case, the *Entry Status* of the record is set to *Inactive*.
If a source node S needs to reuse a route whose status has been set to *Inactive* (i.e. to reactivate a route), it sends an *Activate Route* (ACTR) message towards the destination node D through the route, and intermediate nodes belonging to the path will forward the ACTR to the next hop until it reaches D.
Upon reception of the ACTR message, the destination node changes the status of the corresponding RT entry to *Active,* and replies to the source node with an *Activation OK* message (ACTOK) again following the route. However this time, before forwarding the packet, the intermediate nodes will switch the RT entry to *Active*. Once the ACTOK message reaches the source node S, it also changes the status to *Active* and starts sending data packets.
Since it is always possible that the activation of a route fails, when launching an activation process, the sender sets a time out. If by the end of this time out no ACTOK message is received, the node assumes that the route is broken and triggers a Route Discovery process using the limited flooding scenario.

3.3.3 Route Maintenance

When triggering a *Route Discovery* process and while the RREQ timeout expires, the source node may receive many RREP messages, each one with an alternative route towards the destination node. In general, the order of arrival of these messages will depend only on the number of nodes making up the discovered route: the fewer nodes the route has, the greater the possibility that the

RREP reaches first the destination. However, in terms of energy consumption, fewer nodes do not necessarily imply that the route is the best option.

In LBRA, this situation is treated by accepting subsequent RREP messages and replacing the route if the cost of transmission of the new one is lower. Yet, the source node will start the transmission of data as soon as the first route has been found regardless of whether it is power optimal or not.

The *functional lifetime* of a sensor network can be defined as the period of time after which certain number of nodes has run out of battery, making impossible the completion of the task for which the network was created. Thus, the idea is to find a way to manage the energy so that power depletion is balanced and at any given time, all nodes have on average the same battery level. To accomplish this, we propose to adjust the RREQ packet forwarding based on the remaining battery capacity.

Upon reception of an RREQ message, the node checks its remaining battery level and sets a rebroadcast timer (inversely proportional to the power level) after which the RREQ packet is send to the next hop. Basically, if the forwarding of the RREQ packet is delayed the time required for completing the route increases, which favours high power routes. The delay will be chosen so that the flow of network is not affected and to assure data delivery. Figure 3.6 shows an example of the proposed mechanism.

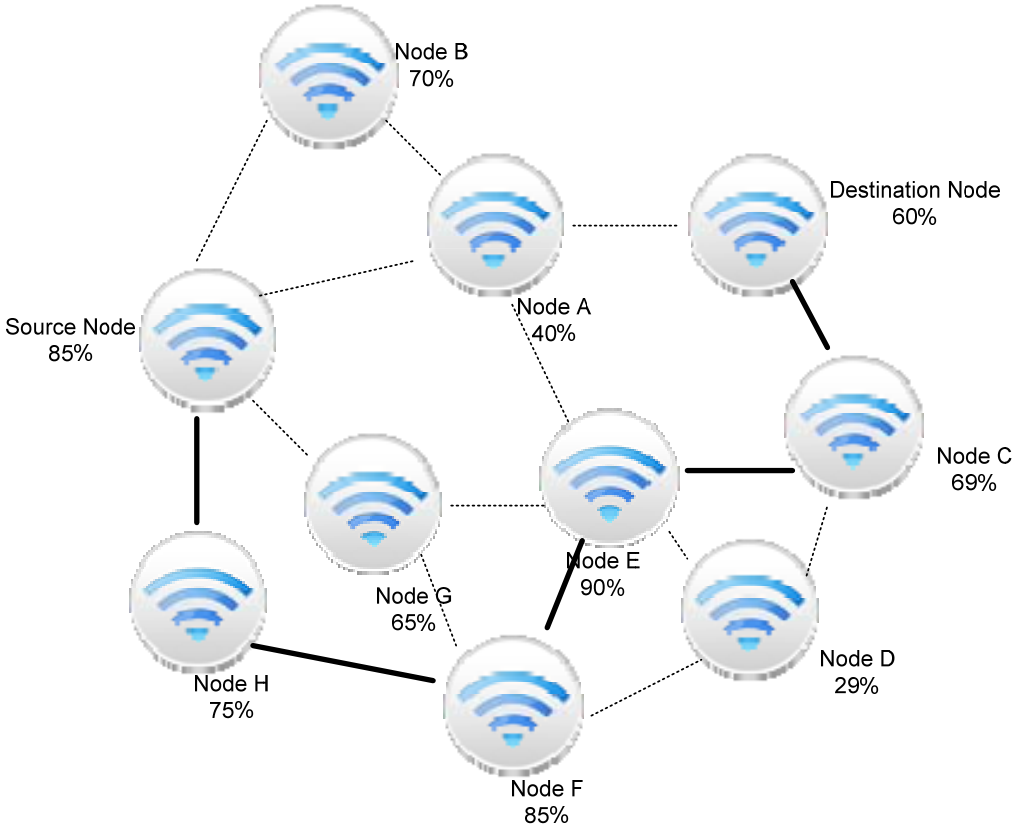


Figure 3.6: Route construction applying RREQ delay

CHAPTER 4 SIMULATION MODEL AND RESULTS

In this chapter we present the simulation model that allows us to evaluate the performance of the LBRA protocol introduced in the previous section. The chapter starts with a detailed description of the model altogether with the basic configuration and closes with the simulation results and their respective analysis.

4.1 Simulation Design

The main purpose of the simulation design is to create an experimentation scenario as realistic as possible in order to carry out a fair performance evaluation of the Location Based Routing Algorithm (LBRA) previously introduced. In order to accomplish this task, we have chosen to use the network simulator (ns), also known as ns-2 in reference to its current generation.

4.1.1 The network simulator

Ns is a discrete event network simulator extensively used in networking research as it provides significant support for simulation of routing and multicast protocols over wired and wireless (local and satellite) networks. Additionally, it is very popular among the networking research community for its extensibility (due to its open source model) and abundant online documentation.

Ns began in 1989 as a variation of the REAL network simulator and has greatly evolved over the past few years. By 1995, *ns* development was supported by DARPA (Defence Advanced Research Projects Agency) through the VINT (Virtual Inter Network Testbed) project at LBL (Lawrence Berkeley National Laboratory) in collaboration with XEROX PARC (Palo Alto Research Center), the UCB (University of California in Berkeley) and the USC/ISI (The Information science institute of the University of Southern California)

Nowadays, *ns* development is supported by DARPA through SAMAN and by NSF (National Science Foundation) through CONSER (Collaborative Simulation for Education and Research), both in collaboration with other researchers and volunteers such as the ICIR, Sun Microsystems and the UCB Daedelus and Carnegie Mellon Monarch projects.

Ns was built in C++ and offers a simulation interface by the means of OTcl, an object-oriented dialect of Tcl (Tool command language). The user describes the desired network topology by

writing OTcl scripts, and then the main *ns* program simulates the topology with the specified parameters. The simulator is event driven and runs in a non-real time fashion [61].

Although it's intended to be simple and easy to use, *ns* is rather complicated for a first time user. Running simulations requires not only good knowledge of the scripting language, but also a fine understanding of *ns* inner operation, which might take quite a long time. Additionally, there are few user-friendly manuals. Even though there's a lot of documentation written by the developers enclosing detailed explanation of the simulator, it is written with the depth of a skilled *ns* user.

4.1.2 Simulation remarks

Since LBRA is an enhanced version of the ZigBee routing, it seems logical and natural to evaluate its performance by comparing the two algorithms. In order to do that, we implemented both protocols and run a series of simulations with the same basic configurations and conditions. At the end, trace files generated by the simulator were analyzed.

For the simulation of the ZigBee routing, we used an existing sample implementation of 802.15.4/ZigBee written by the *ns* developers, and made the required modifications to adjust it to our needs.

As for LBRA, the simulation was not that simple because, even if *ns* is a powerful tool for network simulation, it is an unfinished product and hence, still has many limitations. The main drawback in implementing the protocol as it was proposed was the lack of a sensor network module based on smart antennas, which to the best of our knowledge has not yet being implemented.

In order to overcome this technical hitch, and since the main interest we had in the use of smart antennas was the fact that they provide relative location information for neighbouring nodes, we opted to use the standard antenna model, and take advantage of the simulator's tools to handle location information. It is worth mentioning that this choice doesn't affect the performance evaluation, because we want to appraise the protocol itself and not the impact of using smart antennas.

Additionally, the energy consumption matter was also handled by using the simulator's tools.

From now on we will use the acronym AODV when referring to ZigBee routing, since it is based on the former (with some adjustments as explained in chapter 2).

4.1.3 Basic configuration

The following configuration was defined for the simulation:

- Area: all nodes are generated within an area of 500 x 500 square meters
- Lower layers protocols: the physic (PHY) and MAC layers use the 802.15.4 standard. The transport layer uses UDP
- Antenna: since *ns* doesn't yet have a module for wireless sensor networks based on smart antennas the simulation uses the omni antenna model
- Transmission range: each node can transmit messages in the range of 40 m.
- Traffic load: CBR objects generate packets at a constant bit rate of 0.1Mbps with an interval of 2 ns between packets
- Packet Size: the size of all packets generated is 32 bytes
- Network topologies: random topologies were generated by the means of a program that has the number of nodes as input parameter
- Number of nodes: topologies with 50, 100 and 200 nodes respectively are used in order to evaluate protocol's performance in different circumstances
- Number of sources: 5, 10,18 and 32 sources are used separately
- Simulation time: set to 800 s

4.2 Simulation results and analysis

In this section we carry out an evaluation of LBRA by comparing its performance to that of AODV. Later, we examine the impact of network size and nodes' mobility on the performance of the algorithm by means of simulation results.

4.2.1 Performance evaluation

For the first part of the performance evaluation the topology showed in Figure 4.1 was used:

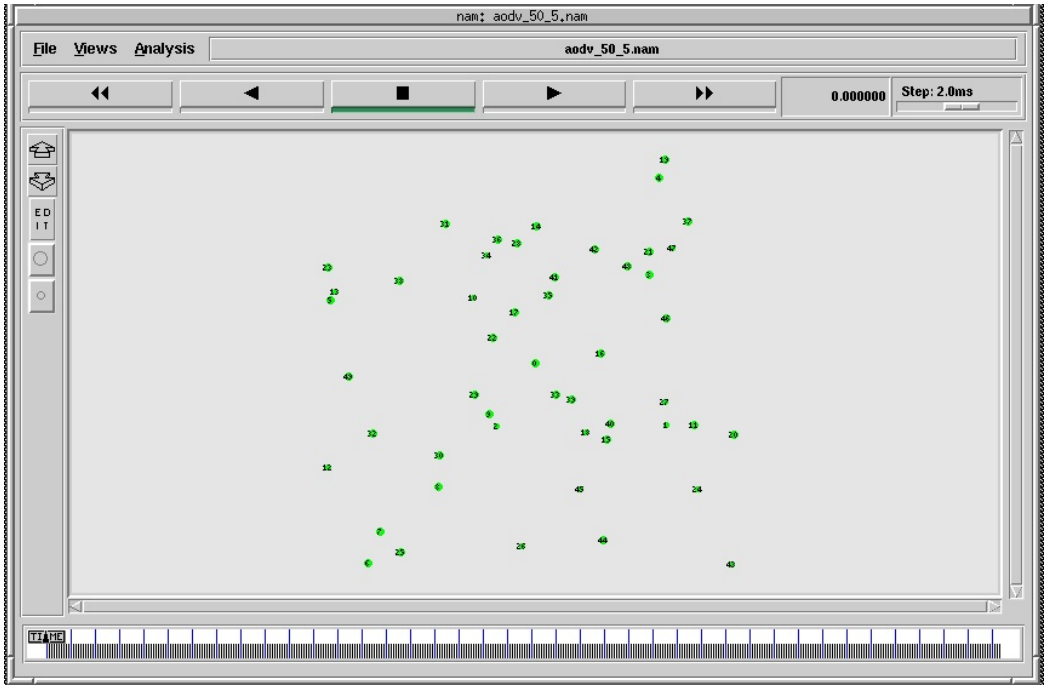
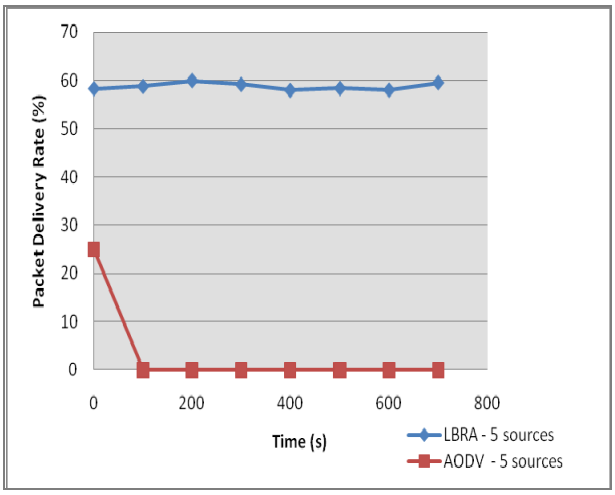


Figure 4.1: Topology 1 with 50 nodes

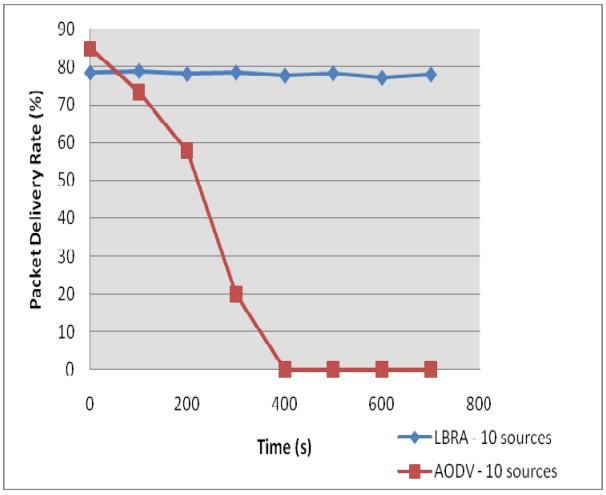
4.2.1.1 Packet Delivery Rate

The *Packet Delivery Rate* is defined as the total number of packets successfully received divided by the total number of packets sent.

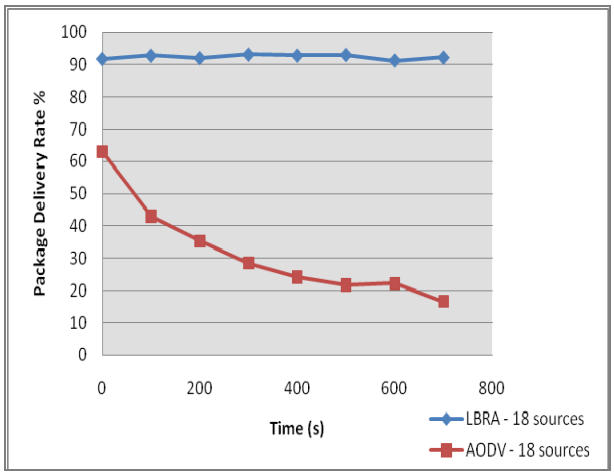
Figure 4.2 shows the experiment results of packet delivery rate. For a better understanding and analysis of the outcomes, let's consider each scenario separately.



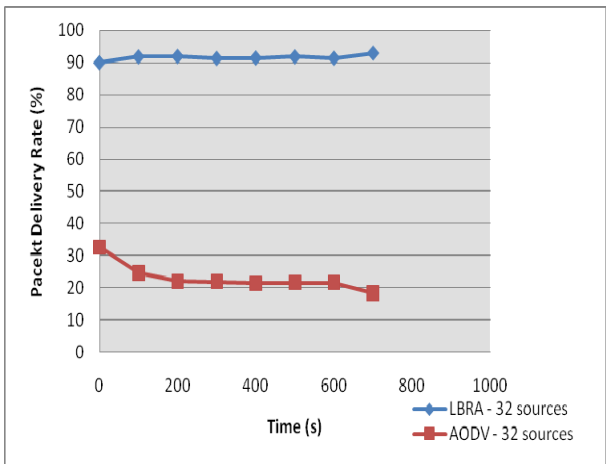
(a)



(b)



(c)



(d)

Figure 4.2: Average packet delivery rate comparison

Figure (a) corresponds to a low traffic load scenario with 5 sources, in which LBRA shows an average delivery rate of 59% that remains stable throughout the simulation. Regarding AODV, the average delivery rate is scarcely 3%, since after the first 100 seconds of simulation no packet reached its destination. However, for this portion of the experiment the average delivery rate is 25%,

Figure (b) also corresponds to a relatively low traffic load scenario with 10 sources and follows the same trend as the previous case: LBRA has an average packet delivery rate of 78% that remains stable throughout the simulation, while AODV's drops rapidly, becoming zero after the first half of the experiment. Although the average delivery rate of the whole simulation for AODV is 34%, if we consider only the first half, this value rises to 59%.

In the normal traffic load scenario with 18 sources shown in Figure (c), LBRA keeps an average packet delivery rate of 92% during the entire simulation. As for AODV, the packet delivery rate decreases as the simulation progresses, reaching an average of 32%.

Finally, in the high traffic load scenario shown in figure (d) with 32 sources, LBRA still has an average delivery rate of 92%, while AODV shows a more stable behaviour than in the other cases, and an average delivery rate of 23%.

As it can be seen, regardless of the number of sources LBRA outperforms AODV, improving its performance as the traffic load increases. Under high traffic load conditions (i.e. scenarios with 18 and 32 sources) LBRA keeps and average packet delivery rate of 92%, while under low traffic load conditions (scenarios with 5 and 10 sources) the packet delivery rate is 59% and 78% respectively.

As for AODV, experiment results show what appears to be an abnormally high packet loss for low traffic load scenarios. However, after a full verification of the initial parameters and settings, several simulations were performed with similar results, which lead us to assume that the protocol does not function well under these kinds of scenarios.

4.2.1.2 Average Routing Overhead

The *Average Routing Overhead* is defined as the total routing control packets divided by the total simulation time.

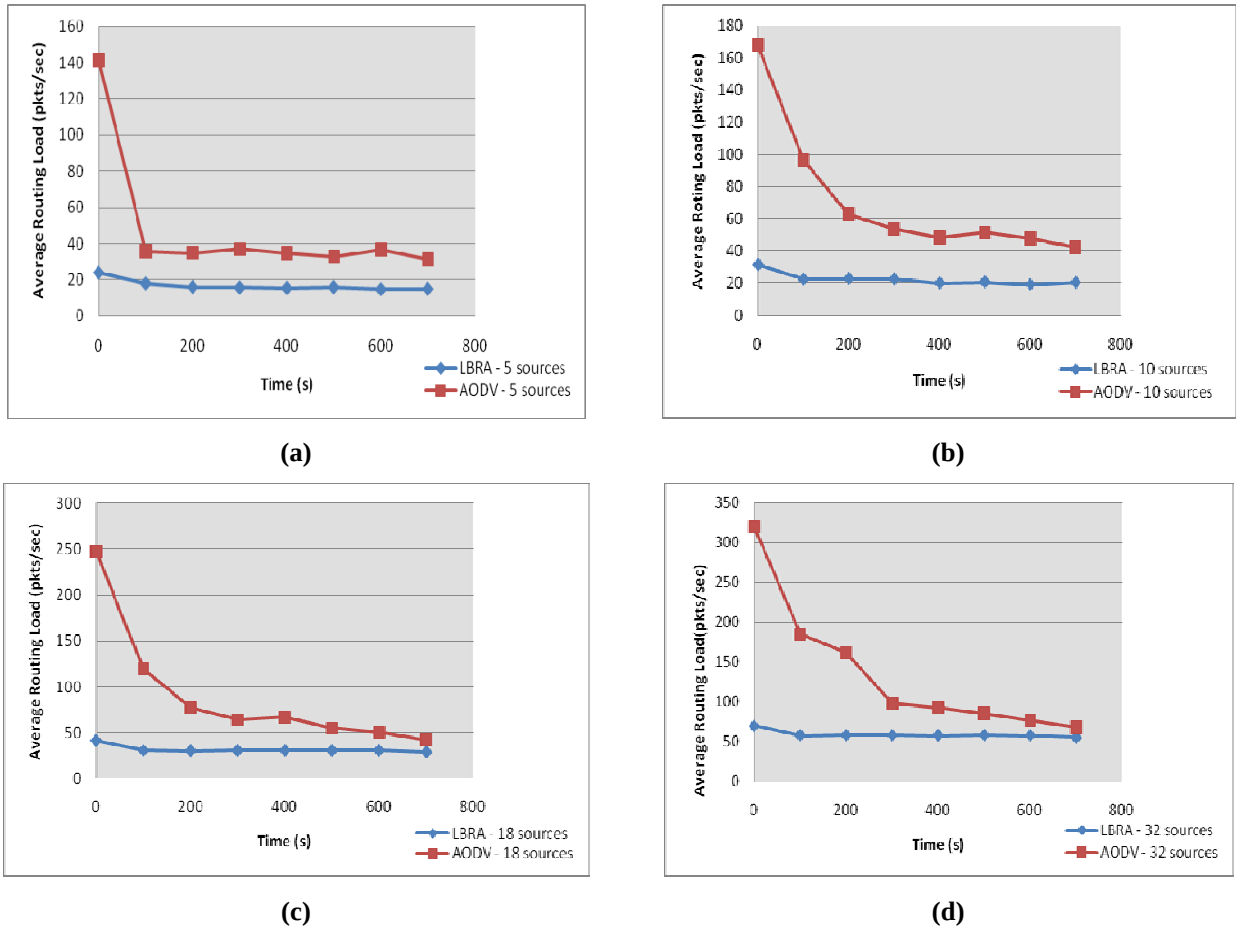


Figure 4.3: Average routing overhead comparison

To analyse the experiment results, let's consider each scenario independently.

Figure (a) illustrates the experiment results for a low traffic load scenario with 5 sources. As seen in the graphic, LBRA shows a steady-state with a slight decrease in the routing load at the beginning of the simulation (in this period occurs the network establishment), and an average routing load of 17 packets per second. Regarding AODV, the routing load drops rapidly in the first portion of the experiment, to stabilize until the end of the simulation. The average routing load is 48 packets per second.

Figure (b) represents the results of the experiment for a relatively low traffic load scenario with 10 sources that follows a similar trend as the previous case: LBRA has a steady-state with a slight decrease in the routing load at the beginning of the simulation, and an average routing load of 23 packets

per second. As for AODV, although the routing load also drops, the reduction is more gradual than in the previous scenario and the average routing load is 71 packets per second.

In Figure (c) (that represents a normal traffic load scenario with 18 sources) and Figure (d) (that corresponds to a high traffic load scenario with 32 sources), both protocols show the same trend as the preceding experiment. In the first case the average routing load for LBRA is 32 packets per second and for AODV is 90 packets per second. In the second case, the average routing load for LBRA is 60 packets per second and for AODV is 136 packets per second.

It is clear from Figure 4.3 that LBRA's performance is superior to that of AODV, confirming that the latter generates more control load (i.e. generates a bigger amount of control packets). The average routing load for LBRA is 33 packets per second, while for AODV is 86. Additionally, it is evident from results that the network establishment takes considerably more time for AODV than for LBRA.

4.2.1.3 Control Overhead

The Control Overhead is defined as the total number of control packets divided by the total number of packets generated.

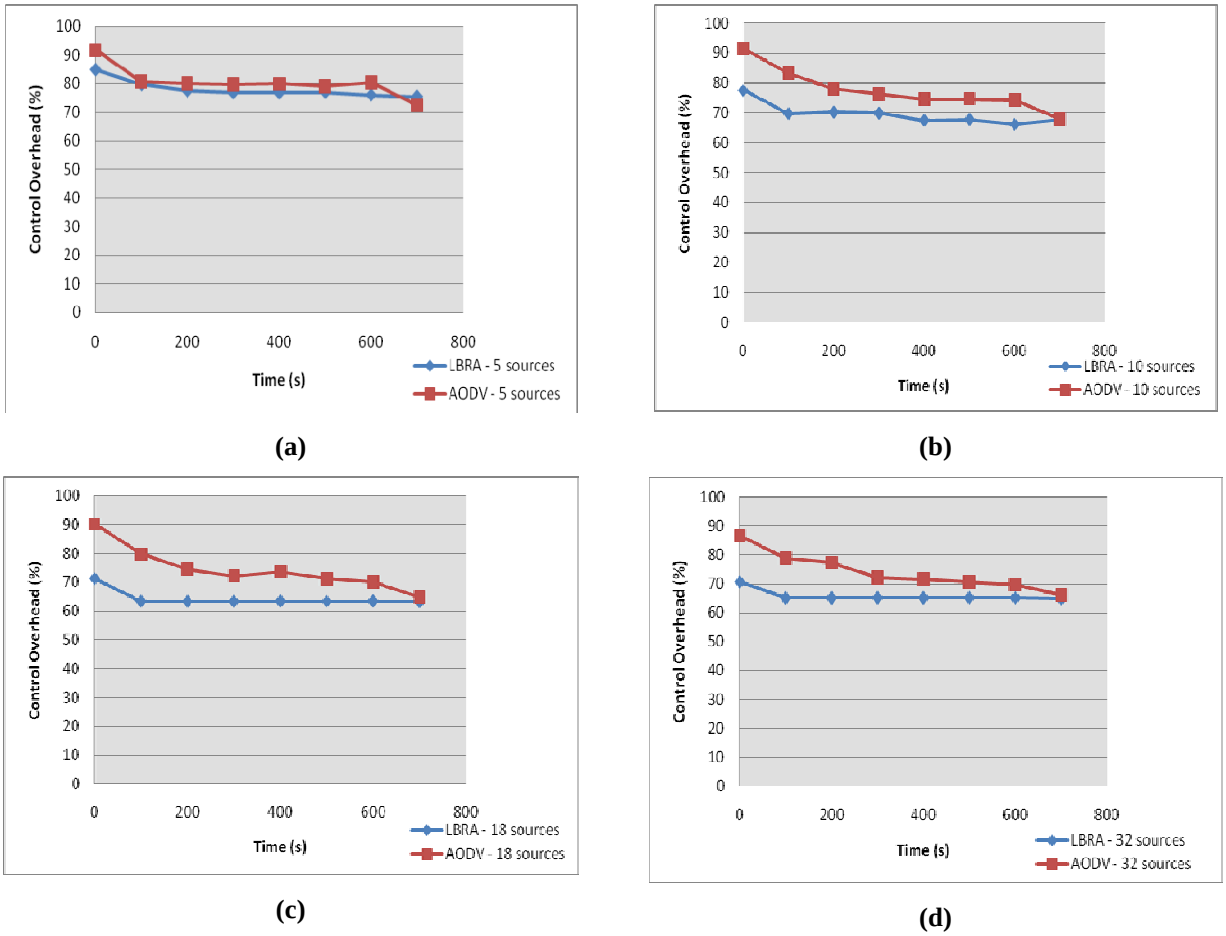


Figure 4.4: Average control overhead comparison

Figure (a) corresponds to the experiment resuls of a low traffic load scenario with 5 sources. As it can be seen, both protocols show the same behaviour: a slight reduction on the control overhead after the first portion of the simulation (where the network establisment is carried out), and a steady-state for the rest of the experiment. For this scenario LBRA has a control overhead of 78% and AODV has a control overhead of 81%.

In the 10 sources scenario (relatively low traffic load) shown in figure (b), the trend is the same as in the previous case. However, the difference in the performance of the two protocols is a bit more pronounced. The average control overhead for LBRA is 70% while for AODV is 78%.

In Figure (c) (showing a normal traffic load scenario witn 18 sources) the average control overhead for LBRA is 64% while for AODV is 75%. As for Figure (d) (correspondig to a high traffic load scenario with 32 sources) the average control overhead for LBRA is 66% and for AODV is 74%.

From Figure 4.4 we notice that LBRA has in general lower control overheads than AODV. For low traffic load scenarios the average control overhead for AODV is 80%, while for LBRA is 74%. Regarding high traffic load scenarios, for LBRA the average value is 65% while for AODV is 75%. These results confirm that both protocols perform better under hight traffic load conditions.

Nevertheless, for an overview of the performance of each of the compared protocols in regard to traffic control, it is necessary to analyse the results shown in Figures 4.3 and 4.4 together. These results, evidence that LBRA not just has a lower control overhead but also, that it generates a smaller amount of control packets than its counterpart.

4.3 Impact of network size on the protocol performance

The number of sensor nodes in a sensor field may be on the order of hundreds or even thousands, depending on the application and the specific purpose of the network. As a consequence, network size and protocol scalability are an important issue when evaluating a protocol performance.

In order to continue with the performance evaluation, additional topologies with 100 and 200 nodes, shown in Figure 4.5 and Figure 4.6 respectively, were considered. The basic configuration and evaluation metrics used in this part are the same as in the previous section.

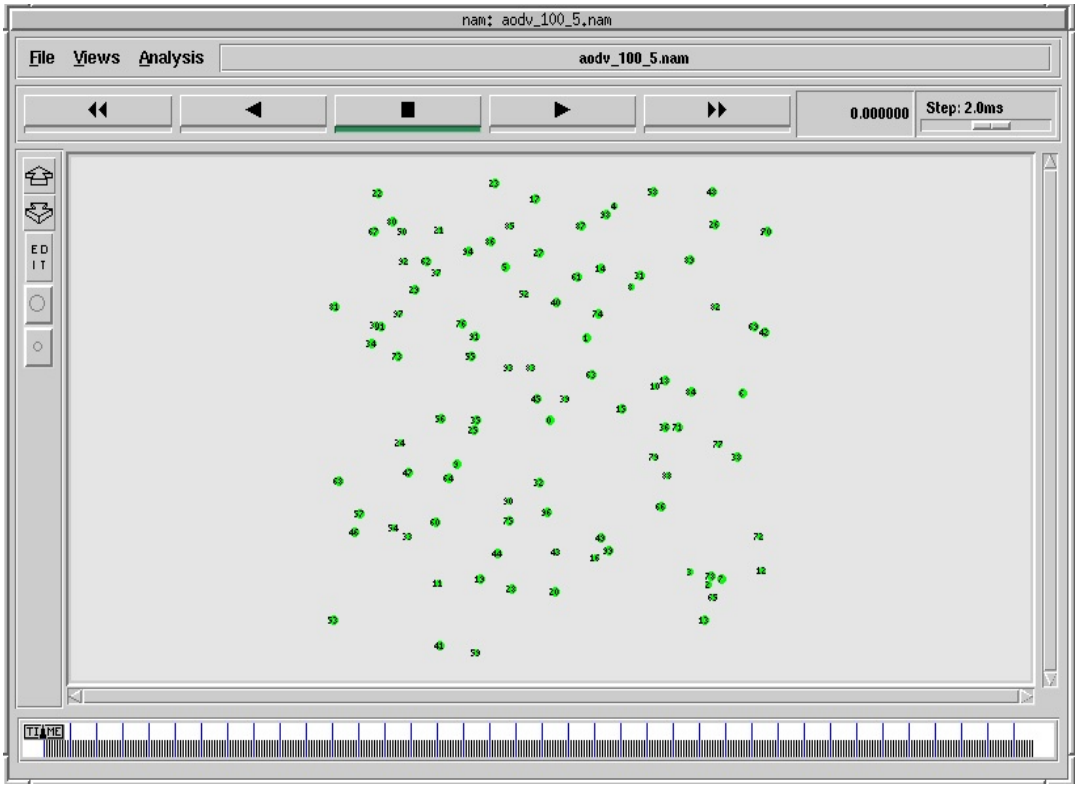


Figure 4.5: Topology with 100 nodes

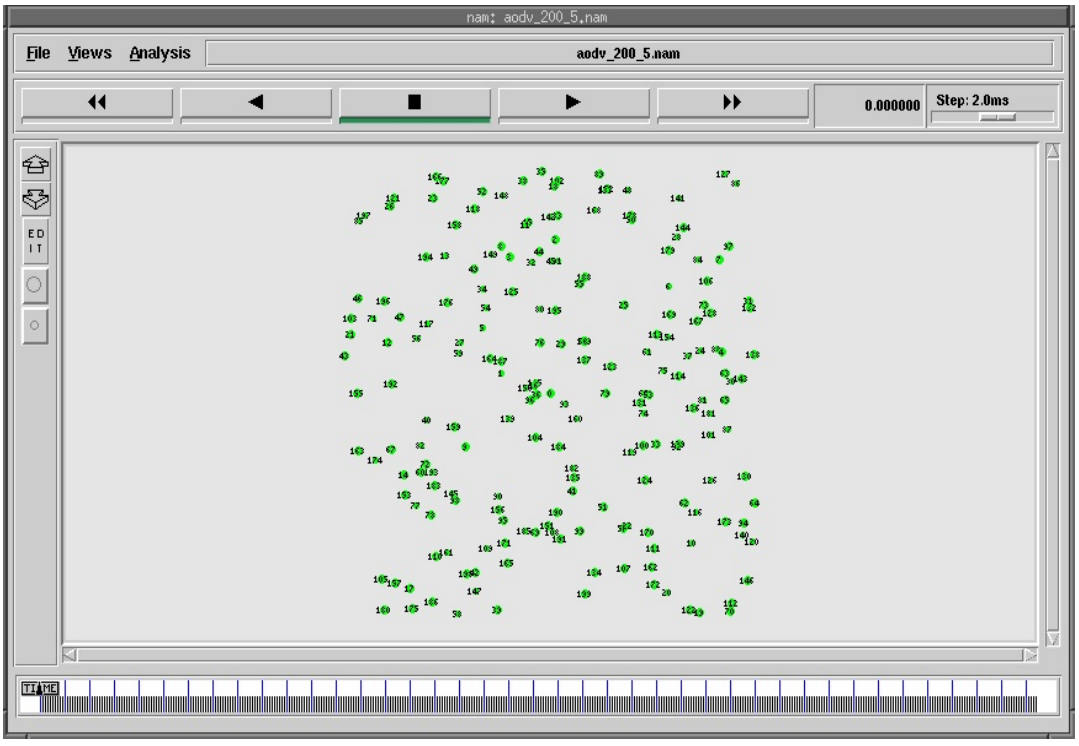


Figure 4.6: Topology with 200 nodes

Packet delivery rate

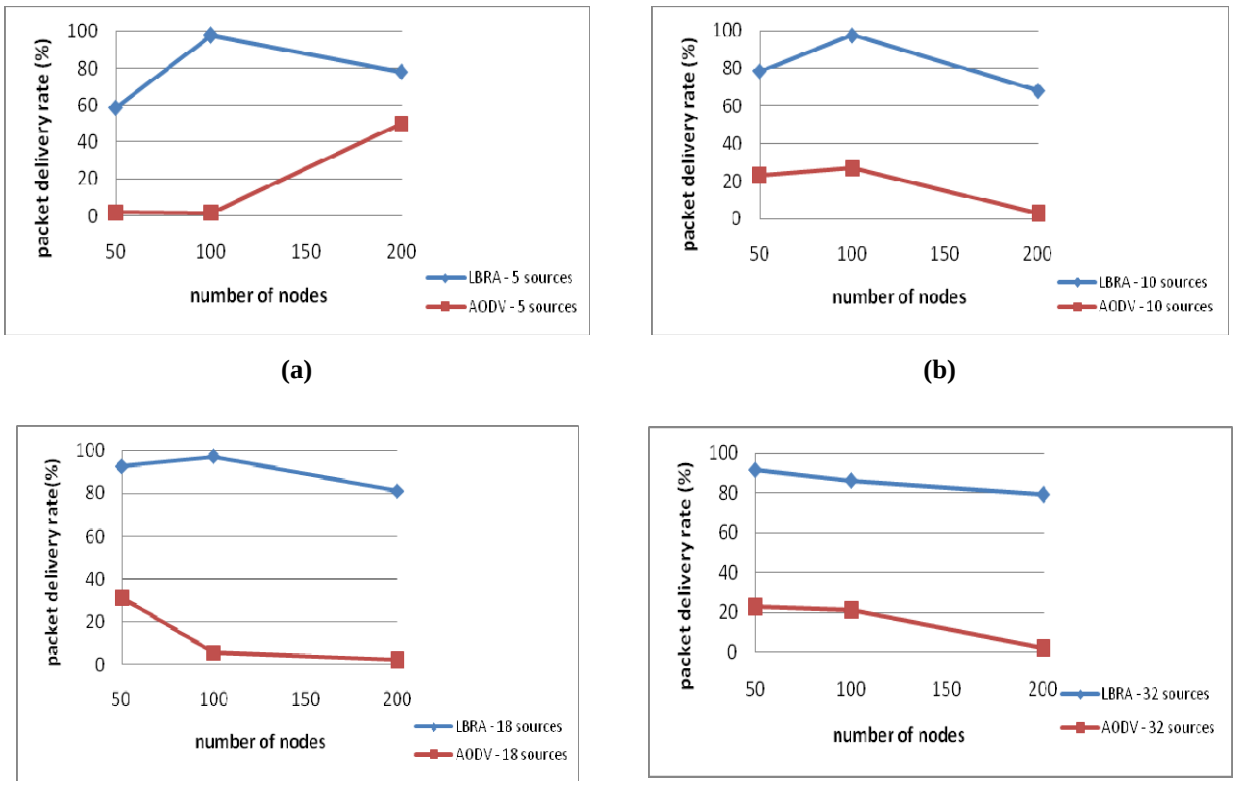


Figure 4.7: Packet delivery rate comparisons for networks with 50, 100 and 200 nodes

Figure (a) shows the experiment results for a low traffic load scenario with 5 sources. Concerning LBRA, we observe that regardless of the number of nodes the protocol registers a good performance. The average packet delivery rate was 58%, 97% and 78% for the topologies with 50, 100 and 200 nodes respectively.

Regarding AODV, the protocol showed a very high packet loss for the first two topologies (with 50 and 100 nodes), reaching an average packet delivery rate of barely 2% in both cases. For the 200 nodes topology the average packet delivery rate was 50%.

Examining Figure (b), which represents the experiment results for a relatively low traffic load scenario with 10 sources, we see that both protocols follow the same trend, reaching their best performance in the medium size topology.

In Figure (c), that illustrates the experiment results for a normal traffic load scenario with 18 sources, LBRA shows the same behaviour as the previous scenarios, while AODV reveals a significant reduction on the average packet delivery rate for the 100 and 200 nodes topologies, reaching values of 5% and 2% respectively.

Finally, in Figure (d), which presents the simulation results for a high traffic load scenario with 32 sources, both protocols show the same trend. In the 200 nodes topology, once again AODV showed a significant packet loss, reaching an average packet delivery rate of 2%.

Concerning packet delivery rate, as seen in Figure 4.7, LBRA outperforms AODV in all cases and in general, both algorithms show the same trend of decreasing its performance as the size of the network increases. It is worth pointing that the packet delivery rate values reached by LBRA are always superiors to 50%.

Control overhead

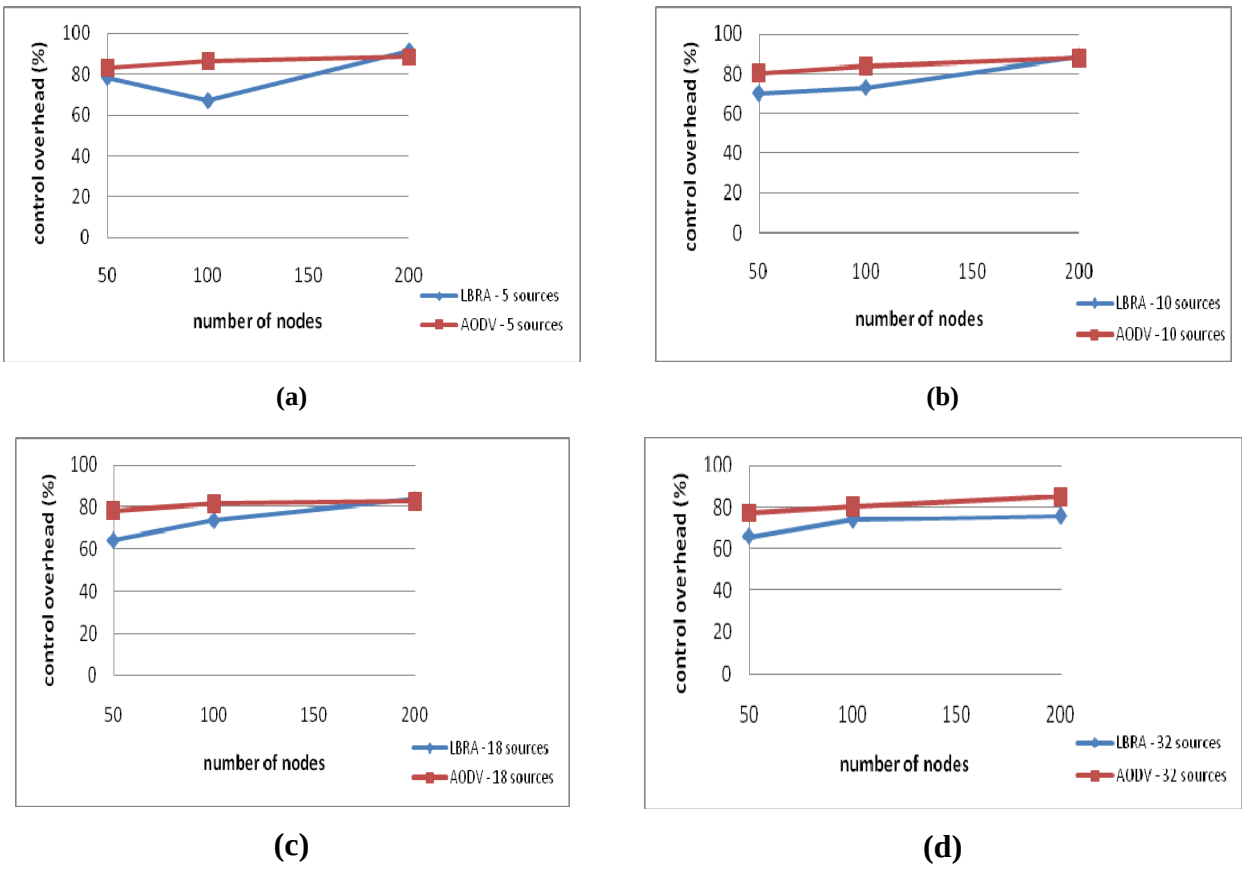


Figure 4.8: Control overhead comparisons for networks with 50, 100 and 200 nodes

Figure (a) illustrates the experiments results corresponding to a low traffic load scenario with 5 sources. As seen in the graphic, LBRA reaches its best performance in the medium size topology and is slightly overcome by AODV in the 200 nodes topology. The average control overhead values for LBRA are 78%, 67% and 91% for the 50, 100 and 200 nodes topologies respectively, while for AODV these values are 83%, 86% and 88%.

In Figure (b), which represents the simulation results for the scenario with 10 sources (relatively low traffic load scenario), the average control overhead for LBRA increases with the number of nodes, and is slightly overcome by AODV in the largest topology. The average control overhead values for LBRA are 70%, 73% and 89% for the 50, 100 and 200 nodes topologies respectively, while for AODV these values are 80%, 84% and 88%.

In Figure (c), which represents the experiment results for a normal traffic load scenario with 18 sources, we observe the same trend as in the previous case: LBRA is slightly overcome by AODV in the largest topology and its average control overhead increases with the number of nodes. The average control overhead values for LBRA are 64%, 74% and 84% for the 50, 100 and 200 nodes topologies respectively, while for AODV these values are 78%, 82% and 83%.

In Figure (d), which presents the simulation results for a high traffic load scenario with 32 sources, we observe a different trend since LBRA outperforms AODV for all network sizes. The average control overhead values for LBRA are 66%, 74% and 76% for the 50, 100 and 200 nodes topologies respectively, while for AODV these values are 77%, 80% and 85%.

Average routing load

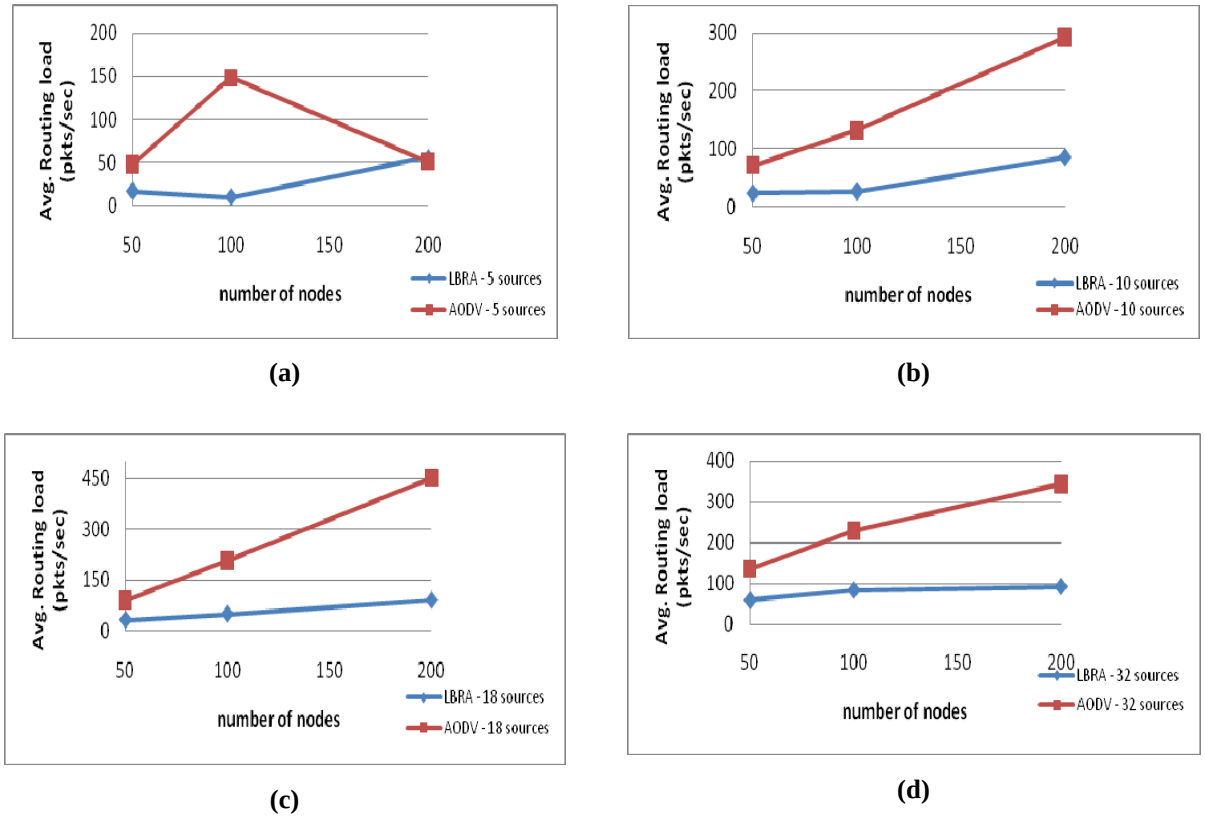


Figure 4.9: Average routing load comparison for networks with 50, 100 and 200 nodes

With the exception of the experiment identified with letter (a), all the scenarios illustrated in Figure 4.9 follow the same trend. In all cases both protocols present a raise in the average routing load as the network size increases, being this raise more significant for AODV.

The difference observed in Figure (a) basically refers to AODV's behaviour, which shows a significant decrease in the routing load for the largest topology, reaching a value close to that obtained in the smallest one. As for LBRA, its behaviour is similar to the one presented in the other scenarios.

In order to have a better understanding of the protocols' performance regarding control traffic, it is necessary to consider Figures 4.8 and 4.9 together, since they provide the whole picture of what is happening within the network. Although AODV seems to outperform LBRA in some scenarios concerning control overhead, LBRA always generates less routing load, which lead us to conclude that it has a better performance.

4.4 Impact of nodes mobility on the protocol performance

As seen in previous chapters, routing requirements may vary depending on the specific purpose of the network and the application. Therefore, another aspect worth considering when performing a protocol evaluation is its flexibility to changing conditions.

It is clear that conceiving an all purpose protocol might be impossible. Nevertheless, it would be nice to know how flexible our protocol is, and to what extent is able to adapt to different needs and requirements.

So far, to carry out the protocol evaluation we have considered only static networks. However, evaluating the impact of nodes mobility on the algorithm performance may result interesting, especially for protocols such as this one, which collect location information and use it to make routing decisions.

4.4.1 Mobility model

The mobility model is designed to describe the movement pattern of mobile nodes, and how their speeds and directions change over the time. Currently there are many different mobility models, being the Random waypoint the most widely used in network research.

Random Waypoint mobility model

Is a random-based mobility model used in mobility management schemes for mobile communication systems. In this model, the position of each MN is randomly selected within a fixed area and then moves to the selected position in linear form with consistent random speed. This movement has time to stop in a period called pause time before starting the next movement. The pause time is determined by model initialization and its speed is uniformly distributed between [0, MaxSpeed][62].

The mobility of Random Waypoint constantly causes topology change. The pause time and the maximum speed determine the mobility behaviour of MNs. If the maximum speed is low and the pause time is high, the network topology becomes relatively stable. On the other hand, if the maximum speed is high and the pause time is small, the network topology is highly dynamic [62].

4.4.2 Mobility simulation results and analysis

In order to measure the impact of nodes mobility on the protocol's performance, once again we used the same scheme as in the previous sections: namely, the basic configuration described in section 4.1.3 together with the 50 nodes topology, the same metrics that have been used so far, and the four scenarios with different traffic loads.

In the first part of this section, we will analyse AODV and LBRA's performance once the nodes start moving, and in the second part the impact of the nodes' speed on the protocols' performance.

For this experiment, the MaxSpeed value was fixed at 1.5 meters per second, and the the max pause value was fixed at 60 seconds.

Packet delivery rate

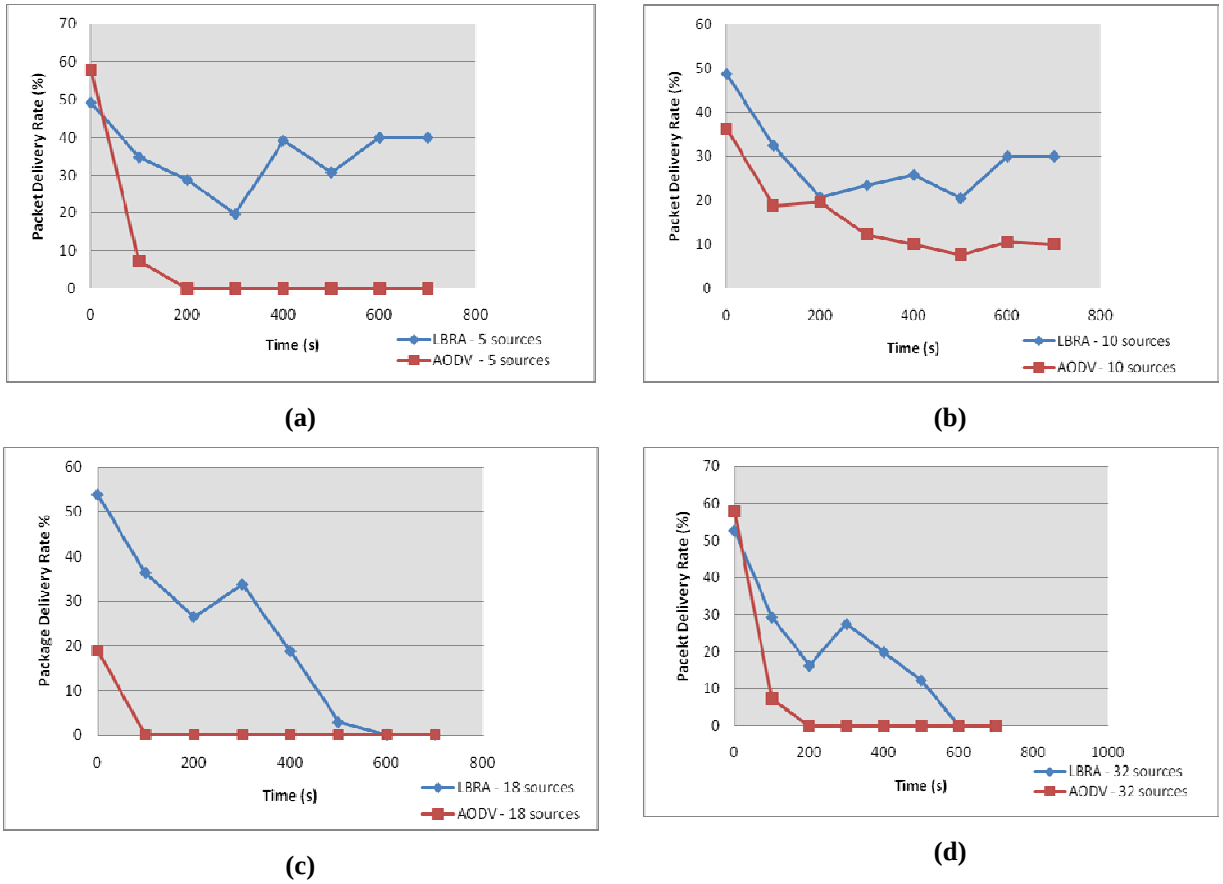


Figure 4.10: Average packet delivery rate comparison for mobile networks

In figures (a), (c) and (d), which correspond to the experiment results for a scenario with low, normal and high traffic load respectively, after the first 100 seconds of simulation, AODV consistently showed a very poor performance and an extremely high packet loss. However, it would be hasty to conclude that this behaviour is due to nodes' mobility, since similar results were obtained in experiments on static networks, as evidenced by Figures 4.2 (a) and 4.2 (b).

Regarding Figure 4.10 (b), which corresponds to the experiment results for a relatively low traffic load scenario with 10 sources, AODV showed a drop in the packet delivery rate at the beginning of the simulation, reaching a state of relative balance towards the end. The average packet delivery rate is 16%.

As for LBRA, in Figures (a) and (b), which present the experiment results for low traffic load conditions, the protocol showed a highly variable behaviour, reaching an average packet delivery rate of 35% and 29% respectively. Under high traffic load conditions, represented in Figures (c) and (d), we observed a drastic decrease in the packet delivery rate as the simulation progresses, until it eventually reached zero. The average packet delivery rate is 21% and 20 % correspondingly.

It is clear from this results that nodes' mobility has a major impact on LBRA's performance, since for the same experiment on static networks the average packet delivery rate was highly superior. Concerning AODV, the impact of nodes' mobility is also evident, although this conclusion is less obvious, given the high packet loss observed in both kind of networks (static and mobile).

Control overhead

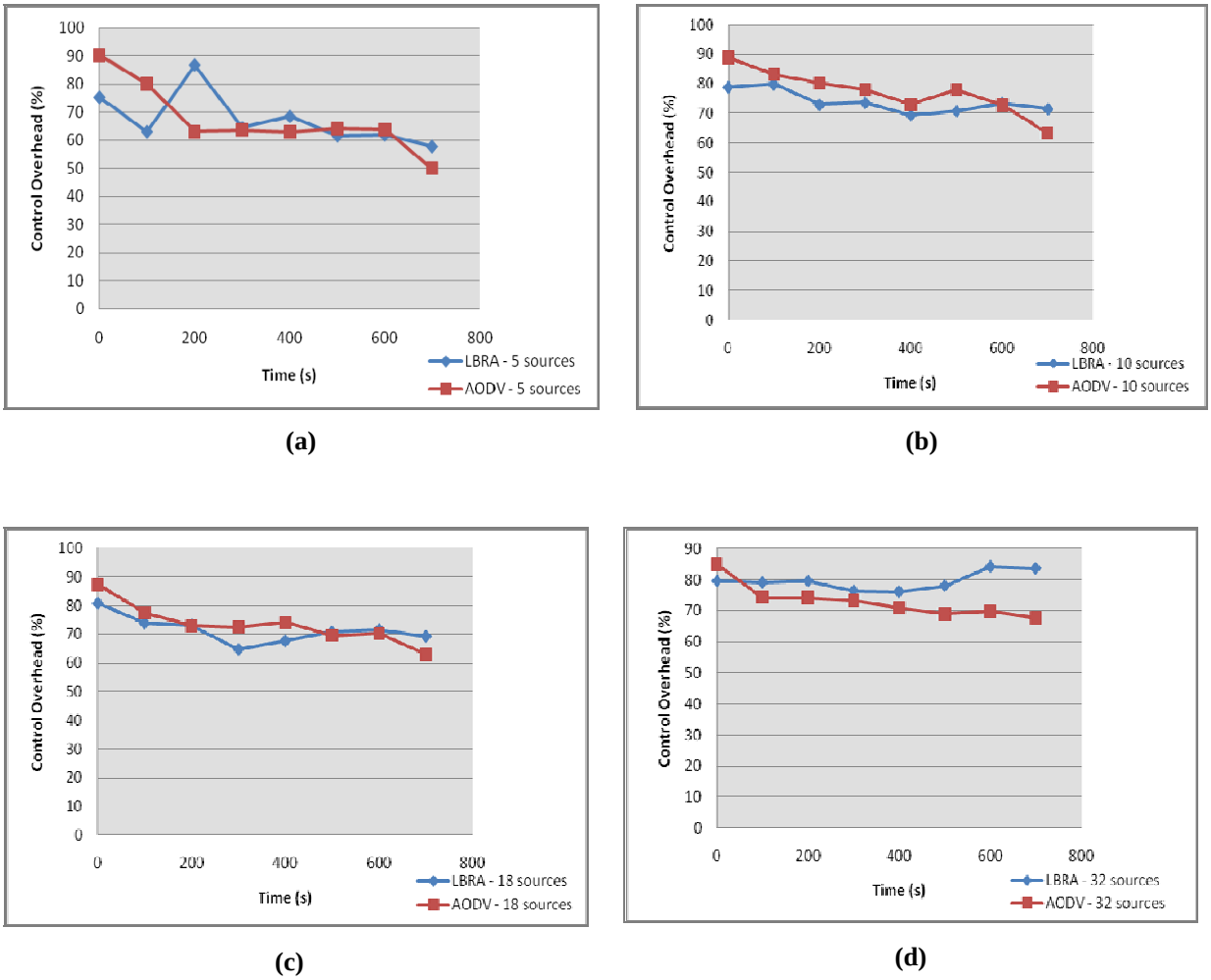


Figure 4.11: Average control overhead comparison for mobile networks

Figure 4.11 shows the experiment results of control overhead.

In the low traffic load scenario presented in Figure (a), LBRA shows a highly variable behaviour and is surpassed by AODV at some stages. In its turn, AODV presents a decrease in the control overhead at the beginning of the simulation and a relative steady behaviour for the rest of the experiment. The average control overhead for both protocols is 67%.

In the scenarios with 10 and 18 transmitting sources, identified in the figure with letters (b) and (c), even though LBRA outperforms AODV, the difference in the control overhead generated by each protocol is small, reaching barely 3% in the worst case-scenario.

Finally, in figure (d), which represents the experiment results for a high traffic load scenario with 32 transmitting sources, AODV shows a better performance than its counterpart. In fact, towards the end of the simulation LBRA exhibits a tendency to increase the control overhead, while

AODV tends to decrease it. The average control overheard for LBRA is 80% and for AODV is 73%.

Comparing the results shown in Figure 4.11 with its counterparts for static networks in Figure 4.4, we observe that node's mobility has a negative impact on LBRA's performance, causing an increase in the average control overhead of up to 5%. In contrast, the average control overhead for AODV remains unchanged.

Average routing load

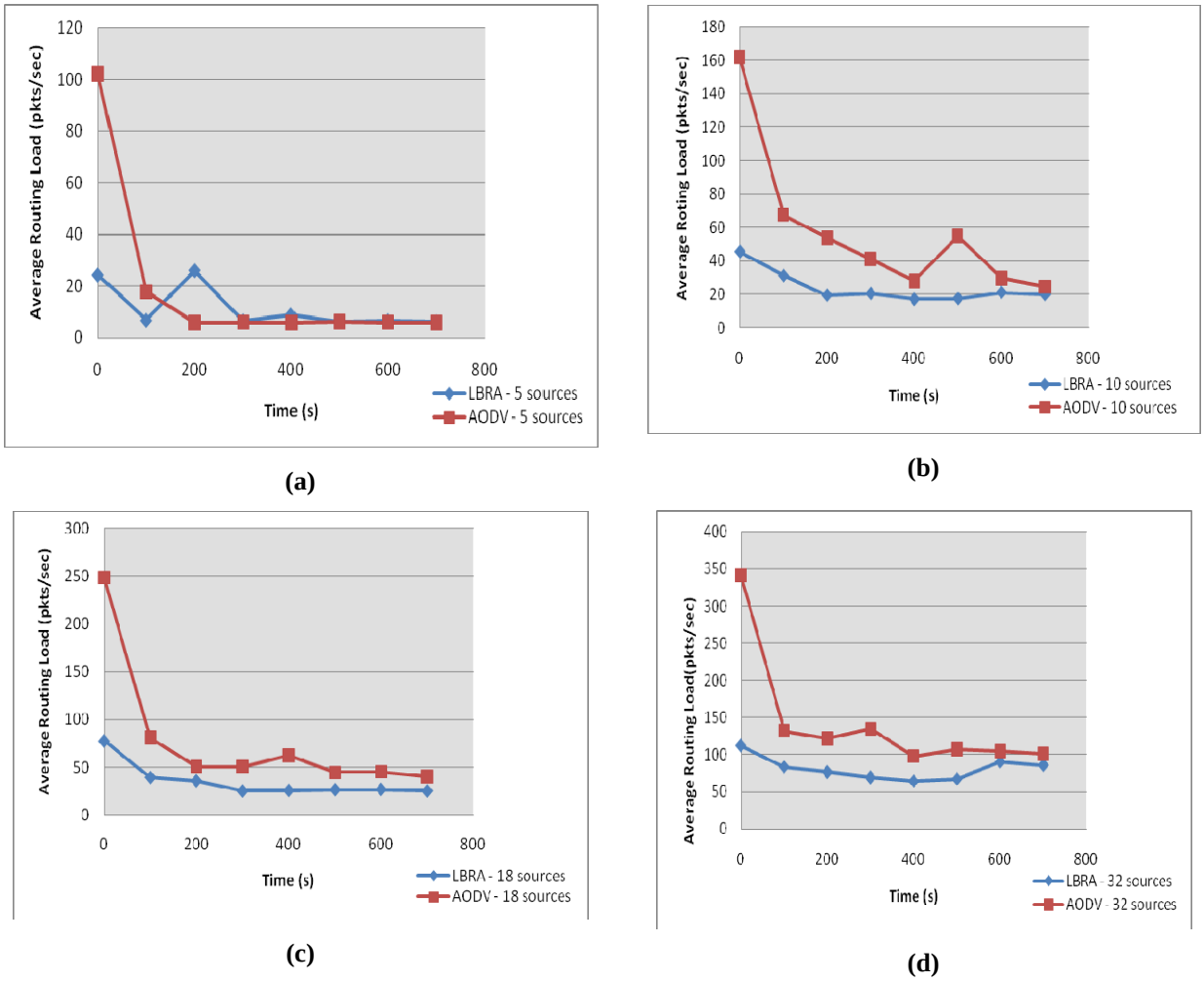


Figure 4.12: Average routing load comparison for mobile networks

Figure 4.12 shows the experiment results of the average routing load. In order to analyse this data, let's consider each protocol separately.

Observing LBRA's behaviour, we notice that the protocol shows a similar trend in all scenarios, that is, a slight decrease in the average routing load at the beginning of the simulation and a relative steady state for the rest of the experiment. As might be expected, the average routing load increased as the number of transmitting sources increased (traffic load).

Concerning AODV, this protocol also shows a similar trend in all scenarios. However, the decrease in the average routing load at the beginning of the simulation is more significant than on LBRA.

Contrasting the results shown in Figure 4.12 with its counterpart for static networks in Figure 4.3, we observe that nodes' mobility didn't have major impact on the average routing load. In fact, the average number of packets per second generated by AODV decreased by approximately 15%, while for LBRA remained practically unchanged.

4.4.3 Impact of speed on performance

In order to measure the impact of speed on protocol's performance, four mobile scenarios with maximum speed fixed at 1.5 m/sec, 5 m/sec, 10 m/sec and 30 m/sec respectively, were used in the simulations. The Max Pause value remained at 60 seconds.

Packet delivery rate

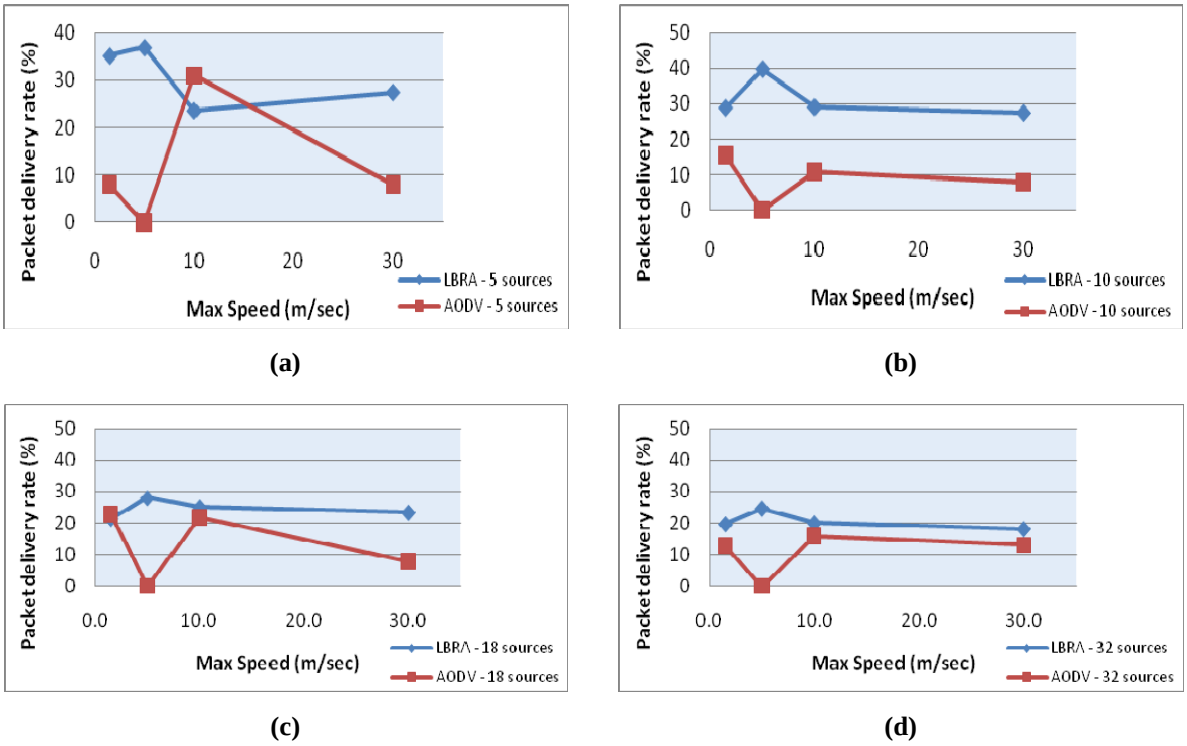


Figure 4.13: Influence of nodes' speed on the average packet delivery rate

In order to analyse the experiment results shown in Figure 4.13, let's consider each protocol separately.

Observing LBRA's performance, we noticed that the protocol shows the same behaviour in all scenarios, reaching its best performance when the maximum speed is 5 m/s. This is because the combination of values chosen as maximum speed and maximum pause, results in a relatively stable topology. For all other Max Speed values, as the speed increased, the average packet delivery rate showed a slight decrease.

Regarding AODV, its behaviour was similar to its counterpart, that is, a slight decrease in the average packet delivery rate as the speed increased. It is worth mentioning that for the mobile scenario with max speed fixed at 5 m/s, once again this protocol presented an extremely high packet loss.

Control overhead

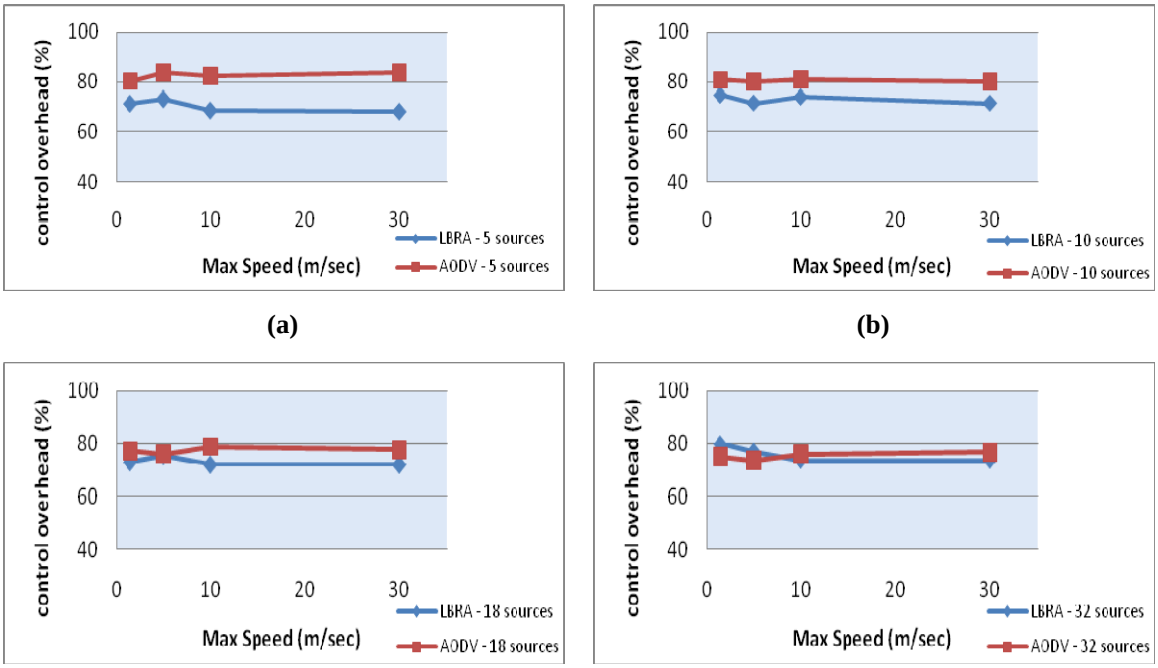


Figure 4.14: Influence of nodes' speed on the average control overhead

As noted in Figure 4.14, the change on the max speed of the nodes doesn't seem to have a major impact on the performance of any of the protocols. In all scenarios and regardless of the number of transmitting sources (traffic load), both protocols showed a rather steady state.

Average routing load

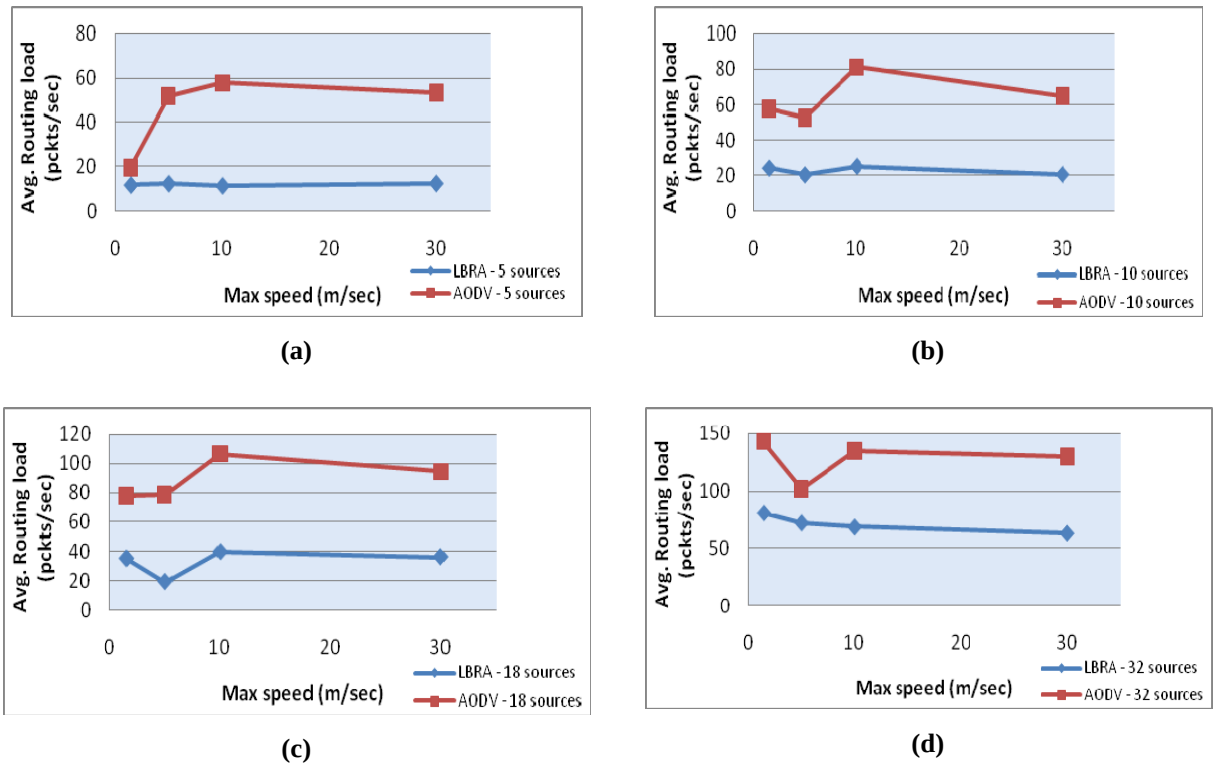


Figure 4.15: Influence of nodes' speed on the average routing load

Finally, when observing the experiments results shown in Figure 4.15, in regards to LBRA, the speed of the nodes doesn't seem to have major impact on the protocols performance: under low, relatively low and normal traffic load conditions, represented by letters (a), (b) and (c) respectively, the average routing remains steady regardless the speed. On the other hand, under high traffic load conditions, represented by letter (d), as the speed increased, the average routing load slightly decreased.

As for AODV, the protocol showed a rather variable behaviour in all scenarios. However, the average routing load tends to slightly increase as the maximum speed value increases.

CHAPTER 5 CONCLUSION

In this chapter we present a summary of the work and contributions made in the context of this thesis, as well as a review of the limitations of research and some guidelines for future work.

5.1 Summary of the work

Wireless sensor networks are an emerging technology that is expected to have a major impact on a wide range of application scenarios in the near future. Nevertheless, these networks have some distinctive characteristics and constraints that make the routing especially challenging.

Due to these special features that distinguish WSNs from contemporary communication networks or wireless ad hoc networks, the use of routing techniques especially designed for these latter is unsuitable.

Once analyzed the WNS's basics and the elements of the routing problem, two key points were established:

1. Routing protocols that do not use geographical location information are not scalable [6].

2. Ideal routing protocols for WSNs should base routing decisions on information exchanged with neighbours, offer network reliability and require minimal message overhead, power consumption and memory footprint [3].

In light of these principles we have proposed the Location Based Routing Algorithm (LBRA) as an alternative for WSNs routing, whose main purpose is to eliminate network control overhead as much as possible.

LBRA is a novel protocol that employs smart antennas to position sensor nodes, uses local position for route decision, implements an original mechanism to collect and synchronize location information and uses node battery information to make power aware routing decisions. It is an enhanced version of the ZigBee routing, which is the current standard for reliable, cost-effective and low power wireless networking, and like the latter is prototyped from AODV.

In order to asses to what extent LBRA truly represents an improvement with respect to the ZigBee routing, a series of simulations were designed with the help of the *Network Simulator (ns)*. Basically, both protocols were implemented in the simulator and its performance was compared in a variety of traffic load, network size and mobility conditions.

The experiment results showed that LBRA succeed in reducing the control overhead and the routing load, improving the packet delivery rate for both static and mobile networks. Additionally, network power depletion is more balanced, since routing decisions are made depending on nodes' battery level.

5.2 Limitations of research

The main limitation of this work is the assumption that the position system is precise enough to fulfill the needs of the algorithm. Smart antennas for wireless sensor systems are a new developing technology that might not be sufficiently advanced to meet the requirements of the algorithm with the desire accuracy. The impact of positioning errors was not explored.

Another limitation is the fact that the additional processing power required by the location estimation algorithm was neglected. Actually, it is a highly complex algorithm that performs multiple calculations, generating computing overhead especially in mobile networks. Furthermore, it is possible that this additional computing activity cause more power consumption, thus shortening network's life.

5.3 Future work

As mentioned may times during this work, routing requirements vary depending on the specific purpose of the network and the application. Therefore, the more adaptability, flexibility and versatility the routing algorithm has, the greater is the number of applications and networks it may serve. For this reason, it would be interesting to develop mechanisms to refine route decisions making the most of location information, in order to be able to guarantee QoS.

In addition to that, as future work would be worthwhile to explore new alternatives to smart antennas for nodes positioning that can offer the same benefits as the latter, but without the limitations identified in the previous section**.**

REFERENCES

[1] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Communications,* vol. 11, pp. 6-28, 2004.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks,* vol. 38, pp. 393-422, 2002.

[3] S. Chessa, P. Baronti, P. Pillai, V. W. C. Chook, A. Gotta, and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards," *Computer Communications,* vol. 30, pp. 1655-95, 2007.

[4] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks,* vol. 3, pp. 325-49, 2005.

[5] I. Stojmenovic, "Position-based routing in ad hoc networks," *IEEE Communications Magazine,* vol. 40, pp. 128-34, 2002.

[6] L. Jinyang, J. Jannotti, D. S. J. De Couto, D. R. Karger, and R. Morris, "A scalable location service for geographic ad hoc routing," Boston, MA, USA, 2000, pp. 120-30.

[7] A. M. Khedr and W. Osamy, "A topology discovery algorithm for sensor network using smart antennas," *Computer Communications,* vol. 29, pp. 2261-8, 2006.

[8] J. N. Ash and L. C. Potter, "Sensor Network Localization via Received Signal Strength Measurements with Directional Antennas," in *the 42nd Annual Allerton Conference on Communication, Control, and Computing*, Champaign-Urbana, IL, September 2004, pp. 1861-1870.

[9] T. Dimitriou and A. Kalis, "Efficient delivery of information in sensor networks using smart antennas," Turku, Finland, 2004, pp. 109-22.

[10] D. Leang and A. Kalis, "Smart SensorDVB: sensor network development boards with smart antennas," Chengdu, China, 2004, pp. 1476-80.

[11] A. Cerpa, J. Elson, D. Estrin, L. Girod, M. Hamilton, and J. Zhao, "Habitat monitoring: application driver for wireless communications technology," *Computer Communication Review,* pp. 20-41, 2001.

[12] P. Bonnet, J. Gehrke, and P. Seshadri, "Querying the physical world," *IEEE Personal Communications,* vol. 7, pp. 10-15, 2000.

[13] P. Johnson and D. C. Andrews, "Remote physiological monitoring in the home," Copenhagen, Denmark, 1996, pp. 63-6.

[14] B. Sibbald, "Use computerized systems to cut adverse drug events: report," *CMAJ: Canadian Medical Association Journal,* vol. 164, p. 1878, 2001.

[15] E. M. Petriu, N. D. Georganas, D. C. Petriu, D. Makrakis, and V. Z. Groza, "Sensor-based information appliances," *IEEE Instrumentation and Measurement Magazine,* vol. 3, pp. 31-5, 2000.

[16] C. Herring and S. Kaplan, "Component-based software systems for smart environments," *IEEE Personal Communications,* vol. 7, pp. 60-1, 2000.

[17] J. M. Rabaey, M. J. Ammer, J. L. da Silva, Jr., D. Patel, and S. Roundy, "PicoRadio supports ad hoc ultra-low power wireless networking," *Computer,* vol. 33, pp. 42-8, 2000.

[18] G. J. Pottie and W. J. Kaiser, "Wireless integrated network sensors," *Communications of the ACM,* vol. 43, pp. 51-8, 2000.

[19] E. Shih, S. Cho, N. Ickes, R. Min, A. Sinha, A. Wang, and A. Chandrakasan, "Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks,"

Proc. of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 272-286, July 2001 2001.

[20] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks,* vol. 52, pp. 2292-330, 2008.

[21] I. F. Akyildiz and E. P. Stuntebeck, "Wireless underground sensor networks: Research challenges," *Ad Hoc Networks,* vol. 4, pp. 669-86, 2006.

[22] I. F. Akyildiz, D. Pompili, and T. Melodia, "Underwater acoustic sensor networks: research challenges," *Ad Hoc Networks,* vol. 3, pp. 257-79, 2005.

[23] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, "A survey on wireless multimedia sensor networks," *Computer Networks,* vol. 51, pp. 921-60, 2007.

[24] A. Bakre and B. R. Badrinath, "I-TCP: indirect TCP for mobile hosts," Vancouver, BC, Canada, 1995, pp. 136-43.

[25] Y. Wei, J. Heidemann, and D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks," *IEEE/ACM Transactions on Networking,* vol. 12, pp. 493-506, 2004.

[26] S. Tilak, N. Abu-Ghazaleh, and W. R. Heinzelman, "A Taxonomy of Wireless Microsensor Network Models," *ACM Mobile Computing and Communications Review,* vol. 6, pp. 28-36, 2002.

[27] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," Los Alamitos, CA, USA, 2000, p. 10 pp. vol.2.

[28] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," New Orleans, LA, USA, 1999, pp. 90-100.

[29] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Computing,* vol. 353, 1996.

[30] ZigBee Alliance, "ZigBee Specifications, version 1.0," April 2005.

[31] Institute of Electrical and Electronics Engineers Inc., "IEEE Std. 802.15.4-2003. Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Persona Area Networks (LR-WPANs)," *IEEE Press,* October 1, 2003.

[32] W. R. Heinzelman, J. Kulik, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," Seattle, WA, USA, 1999, pp. 174-185.

[33] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed diffusion for wireless sensor networking," *IEEE/ACM Transactions on Networking,* vol. 11, pp. 2-16, 2003.

[34] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," Boston, MA, USA, 2000, pp. 243-54.

[35] F. Qing, G. Jie, and L. J. Guibas, "Locating and bypassing routing holes in sensor networks," Hong Kong, China, 2004, pp. 2458-68.

[36] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for Ad Hoc routing," in *International Conference on Mobile Computing and Networking*, Rome, Italy, 2001, pp. 70 - 84.

[37] J. S. Blogh and L. Hanzo, *Third-Generation Systems and Intelligent Wireless Networking: Smart Antennas and Adaptive Modulation*: Halsted Press, 2002.

[38] J. Litva and T. K. Lo, *Digital Beamforming in Wireless Communications*: Artech House, Inc., 1996.

[39] The International Engineering Consortium, "Smart Antenna Systems," in *Web ProForums*, pp. 1-29.

[40] R. T. Compton, *Adaptive Antennas: Concepts and Performance*. Englewood Cliffs, NJ: Prentice Hall, 1988.

[41] M. Chryssomallis, "Smart antennas," *IEEE Antennas and Propagation Magazine,* vol. 42, pp. 129-36, 2000.

[42] A. Kalis and T. Antonakopoulos, "Direction finding in IEEE802.11 wireless networks," *IEEE Transactions on Instrumentation and Measurement,* vol. 51, pp. 940-8, 2002.

[43] J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," New York, NY, USA, 1998, pp. 85-97.

[44] S. R. Das, C. E. Perkins, and E. M. Royer, "Performance comparison of two on-demand routing protocols for ad hoc networks," Piscataway, NJ, USA, 2000, pp. 3-12.

[45] A. Boukerche, "Performance evaluation of routing protocols for ad hoc wireless networks," *Mobile Networks and Applications,* vol. 9, pp. 333-42, 2004.

[46] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, and M. Degermark, "Scenario-based performance analysis of routing protocols for mobile ad-hoc networks," New York, NY, USA, 1999, pp. 195-206.

[47] P. K. K. Loh, H. Wen Jing, and P. Yi, "Reliable and efficient communications in sensor networks," *Journal of Parallel and Distributed Computing,* vol. 67, pp. 922-34, 2007.

[48] A. Hac, *Wireless Sensor Network Design*. New York: John Wiley & Sons, Ltd., 2003.

[49] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security protocols for sensor networks," 2001, pp. 189-199.

[50] K. Yongjin, L. Jae-Joon, and H. Ahmed, "Modeling and analyzing the impact of location inconsistencies on geographic routing in wireless networks," *SIGMOBILE Mob. Comput. Commun. Rev.,* vol. 8, pp. 48-60, 2004.

[51] S. Biaz and J. Yiming, "A survey and comparison on localisation algorithms for wireless ad hoc networks," *International Journal of Mobile Communications,* vol. 3, pp. 374-410, 2005.

[52] S. Zhilong and T. S. P. Yum, "Precise localization with smart antennas in ad-hoc networks," Piscataway, NJ, USA, 2007, pp. 1053-7.

[53] A. Quintero, D. Y. Li, and H. Castro, "A location routing protocol based on smart antennas for ad hoc networks," *Journal of Network and Computer Applications,* vol. 30, pp. 614-636, 2007.

[54] J. Liberti and T. S. Rappaport, *Smart Antennas for Wireless Communications: IS-95 and Third Generation CDMA Applications*, 1 ed.: Prentice Hall, 1999.

[55] H. L. Van Trees, *Optimum Array Processing (Detection, Estimation, and Modulation Theory, Part IV)*. New York: Wiley Interscience, 2002.

[56] R. Roy and T. Kailath, "ESPRIT-estimation of signal parameters via rotational invariance techniques," *Optical Engineering,* vol. 29, pp. 296-313, 1990.

[57] R. O. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE Transactions on Antennas and Propagation,* vol. AP-34, pp. 276-80, 1986.

[58] S. Haykin, *Adaptive Filter Theory*, 4 ed.: Prentice Hall, Sep 24 2001.

[59] K. Young-Bae and N. H. Vaidya, "Location-aided routing (LAR) in mobile ad hoc networks," *Wireless Networks,* vol. 6, pp. 307-21, 2000.

[60] J. C. de Oliveira, F. S. Cohen, and E. Taslidere, "Locating hot nodes and data routing for efficient decision fusion in sensor networks," *Ad Hoc Networks,* vol. 4, pp. 416-30, 2006.

[61] "The Network Simulator - ns-2 - http://www.isi.edu/nsnam/ns/."

[62] J. Ariyakhajorn, P. Wannawilai, and C. Sathitwiriyawong, "A comparative study of random waypoint and Gauss-Markov mobility models in the performance evaluation of MANET," Piscataway, NJ, USA, 2006, pp. 894-9.